НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

«На правах рукопису»

УДК 004.056

«До захисту допущено»
В.о. завідувача кафедри
_____ М.В.Грайворонський
“___”_____2019 р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності: 125 Кібербезпека
на тему: Оцінка захищеності SCADA систем на основі функцій правдоподібності

Виконав (-ла): студент (-ка) ____ курсу, групи _____
(шифр групи)

Шевчук Ірина Борисівна _____
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник к.т.н., доц. Коломицев Михайло Володимирович _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2019 року

Реферат

Представлена робота має обсяг 75 сторінок, містить 7 ілюстрацій, 15 таблиць та 8 літературних посилань.

Метою даної роботи є підвищення ефективності захисту SCADA системи шляхом виявлення слабких місць системи та оцінки рівня її захищеності за допомогою розробленого підходу, основаного на функції правдоподібності, який допомагає оцінити рівень захищеності з різних сторін та отримати найбільш детальну картину щодо безпеки системи.

Об’єктом дослідження є стан захищеності SCADA систем.

Предметом дослідження є методи і підходи до оцінки захищеності SCADA та виявлення найбільш ефективних з них.

Результатом роботи є розроблений підхід, що дозволяє визначити рівень захищеності SCADA систем на основі функції правдоподібності. Суть підходу в тому, що він складається з чотирьох основних кроків, в результаті яких отримуються якісні/ кількісні дані, необхідні для визначення загальної оцінки захищеності SCADA системи. Результати роботи представлені у вигляді рисунків та таблиць.

Методи дослідження: ознайомлення та опрацювання літератури, що представлено монографічними та журнальними матеріалами, електронними ресурсами, які стосуються досліджуваної теми, аналіз різних способів перевірки безпеки SCADA систем, структурування отриманих результатів.

Результати роботи можуть бути використані для визначення рівня захищеності SCADA системи, виявлення проблем безпеки та здійснення порівняльної характеристики початкового стану безпеки SCADA системи та стану системи після виправлення знайдених недоліків.

Ключові слова: SCADA, ризик, захищеність, сценарії безпеки, атаки, підхід, функція правдоподібності.

Abstract

The presented work has 75 pages, 7 figures, 15 tables and 8 literary references.

The aim of this qualification is to increase the efficiency of SCADA protection by detecting weaknesses in the system and assessing its security through a feasibility-based approach, which helps to assess the level of protection from different parties and obtain the most detailed picture of the security of the system.

The object is security status of SCADA system.

The subject of the study is methods and approaches to assessing the security of SCADA and identifying the most effective of them.

The result of the work is a developed approach that allows determining the level of security of the SCADA system based on the likelihood function. The essence of the approach is that it consists of three main steps, at the output of which the qualitative / quantitative data necessary for the overall assessment of the security of the SCADA system are formed. The results of the work are presented in the form of drawings and tables.

Methods of research: familiarization and processing of literature, presented by monographic and journal materials, electronic resources related to the topic under study, analysis of various methods for testing the safety of SCADA systems, structuring the results obtained.

The results of the work can be used to determine the level of security of the SCADA system, the identification of security problems and the comparative characteristics of the initial state of the safety of the SCADA system, and after correction of the defects found in the system.

Keywords: SCADA, risk, protection, safety scenarios, attacks, approach, likelihood function.

ЗМІСТ

Перелік умовних позначень, символів, одиниць, скорочень термінів 7
Вступ 8
1 Безпека SCADA систем 11
1.1 Особливості автоматизованої системи SCADA 11
1.2 Атаки та вразливості SCADA систем 17
Висновки до розділу 1 20
2 Аналіз способів оцінки захищеності систем 21
2.1 Тестування на проникнення 21
2.2 Оцінка захищеності SCADA системи на основі 5 етапів 23
2.3 Формальна модель оцінки захищеності АСУ ТП 25
Висновки до розділу 2 26
3 Підхід до оцінки захищеності SCADA систем 27
3.1 Основні етапи підходу до оцінки захищеності SCADA систем 28
3.2 Розрахунок оцінки захищеності SCADA системи 65
3.3 Практичне застосування підходу до оцінки захищеності 65
Висновки до розділу 3 71
Висновки 73
Перелік джерел послань 75

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ ТЕРМІНІВ

SCADA – Supervisory Control And Data Acquisition System;

АСУ ТП – автоматизована система управління технологічним процесом;

PLC – Programmable Logic Controller

XSS – Cross Site Scripting;

SQL – Structured Query Language;

ОС – операційна система;

ПЗ – програмне забезпечення;

CSRF – Cross Site Request Forgery;

IDS – Intrusion Detection System;

IPS – Intrusion Prevention System;

NIST – National Institute of Standards and Technology;

ISA – Industry Standard Architecture;

SSL – Secure Sockets Layer.

ВСТУП

Керування атомними і гідроелектростанціями, нафто- і газопроводами, заводами, транспортними мережами (метро і швидкісними потягами), а також багато іншими життєво важливих для людства систем здійснюється за допомогою різних комп'ютерних технологій.

Сучасна АСУ ТП (автоматизована система управління технологічним процесом) являє собою багаторівневу людино-машинну систему управління. Створення АСУ здійснюється з використанням автоматичних інформаційних систем збору даних і обчислювальних комплексів, які постійно удосконалюються по мірі еволюції технічних засобів і програмного забезпечення. Проте зі збільшенням технічних засобів в SCADA система зростає і кількість вразливостей в них. Дані вразливості можуть використовуватися кіберзлочинцями, особливо зважаючи на те, що на сьогоднішній день кіберзлочинність розвинена як ніколи і будь-який зловмисник у мережі може легко залишатися абсолютно анонімним.

Питання захищеності SCADA систем гостро постало після ряду інцидентів зв’язаних з шкідливими програми, такими як Stuxnet, Flame, DQ, і т.д.

Ще однією великою проблемою є незахищеність більшості протоколів обміну даними між SCADA та PLC, які взагалі не мають на увазі якусь аутентифікацію і авторизацію користувача або обладнання, що призводить до наступного: будь-який пристрій, який з’явився в технологічному ланцюгу може не тільки отримувати, але й видавати керуючі команди на будь-який інший пристрій в даній мережі.

Також не сприяють поліпшенню ситуації і самі виробники ПЗ SCADA, найчастіше вони записують службові логіни і паролі, SSH і SSL ключі в сам програмований логічний контролер, що може сприяти заміні компонентів системи зловмисниками. Також розробники в більшості випадків закладають апаратні і програмні можливості віддаленого адміністрування, проте конфігурація цих параметрів однозначно не визначається ними, залишаючи цей вибір за кінцевим користувачем. В

свою чергу користувач часто нехтує такими налаштуваннями та залишає їх за замовчуванням, внаслідок чого, вся система доступна з інтернету, і є можливість несанкціонованого підключення до неї та зміни параметрів всієї системи в цілому.

Зважаючи на ці недоліки, можна зробити висновок, що сучасні SCADA системи дуже вразливі перед кіберзлочинцями та можуть бути скомпрометовані з метою крадіжки конфіденційної або комерційної інформації. Ще одним варіантом розвитку ситуації є те, що можуть бути внесені критичні зміни в функціонал системи з метою відмови всього технологічного обладнання і в результаті поломки, можуть неправильно інформуватись оператори з метою прийняття неправильних рішень, які згодом приведуть до аварійних ситуацій.

Тому, для того щоб максимально забезпечити безпеку, необхідно спочатку оцінити рівень захищеності SCADA систем та виявити потенційно вразливі місця в системі.

Актуальність даної роботи полягає в тому, що в ній висвітлюються проблеми безпеки SCADA систем. В залежності від того, яка мета переслідується, використовується один із способів для перевірки захищеності SCADA систем, що існують на даний момент. Проте, зважаючи на загрози, що можливі для цих систем, зазвичай необхідно застосовувати комплекс перевірок. На даний момент не існує єдиного методу визначення рівня захищеності SCADA систем, який би дозволяв визначати проблеми з різних сторін. В даній роботі представлено підхід до оцінки, який охоплює декілька аспектів безпеки SCADA систем.

Метою даної роботи є підвищення ефективності захисту SCADA системи, шляхом виявлення слабких місць системи та перевірки її рівня захищеності на основі аналізу та оцінки системи зі сторони ‘safety’ та ‘security’.

Завдання, які були поставлені при виконанні даної роботи:

- аналіз основних аспектів безпеки SCADA систем;
- пошук та аналіз найпоширеніших способів перевірки захищеності SCADA систем;

- створення підходу до оцінки захищеності SCADA систем на основі функції правдоподібності, яка допомагає оцінити рівень захищеності з різних сторін та отримати найбільш детальну картину щодо системи, яка використовується;
- опис кожного з етапів підходу та їхня роль в загальній оцінці захищеності;
- оцінка реальної SCADA системи на основі розробленого підходу.

Об'єктом дослідження є перевірка стану захищеності SCADA систем.

Предмет дослідження – методи і засоби тестування безпеки SCADA систем та виявлення найбільш ефективних з них.

Методами дослідження: ознайомлення та опрацювання джерел літератури, що стосуються даної теми, аналіз різних способів перевірки SCADA систем, структурування отриманих результатів.

Наукова новизна даної роботи полягає в тому, що вперше було запропоновано підхід до оцінки захищеності SCADA систем на основі функції правдоподібності, який дозволяє отримати ширшу картину щодо проблем безпеки даного типу систем. Розроблений підхід дозволяє визначити рівень захищеності SCADA системи, що перевіряється. Він основується на чотирьох основних етапах, на виході кожного з яких формуються кількісні/якісні дані, необхідні для обчислення оцінки захищеності SCADA системи.

Результуюча оцінка захищеності залежить від наступних критеріїв:

1. описаних 'safety' і 'security' подій, які входять в небажані сценарії;
2. оцінки функції правдоподібності сценарії безпеки 'safety' та 'security';
3. оцінки збитку, отриманого в результаті реалізації сценаріїв;
4. оцінки ризику, отриманого в результаті реалізації сценаріїв.

Практичне значення результатів підхід до оцінки захищеності SCADA системи на основі функції правдоподібності полягає у практичному застосуванні результатів дослідження для виявлення проблем безпеки SCADA системи, визначення поточного рівня захищеності системи, та порівняльної характеристики початкового стану безпеки та після виправлення знайдених недоліків системи.

1 БЕЗПЕКА SCADA СИСТЕМ

1.1 Особливості автоматизованої системи SCADA

В теперішній час внаслідок глобального поширення комп’ютерних систем в галузі автоматизації промислових процесів все частіше застосовуються системи збору даних і оперативного диспетчерського управління (SCADA – Supervisory Control And Data Acquisition System). SCADA – це тільки один з компонентів автоматизованих систем управління, які на сучасному етапі є складним комплексом програмних і апаратних засобів.

Переважна більшість автоматизованих систем управління будується на базі промислових контролерів, які є первинними засобами збору, обробки інформації, регулювання технологічними параметрами, аварійної сигналізації, захисту і блокування (нижній рівень системи). Оброблена контролерами інформація передається до комп'ютеризованих систем, які є робочим місцем оператора-технолога, де відбувається подальша обробка даних процесу і представлення оператору в інтуїтивно зрозумілому вигляді (верхній рівень АСУ ТП).

SCADA-системи в ієрархії програмно-апаратних засобів промислової автоматизації знаходяться на верхньому рівні. Якщо спробувати стисло охарактеризувати основні функції, то можна сказати, що SCADA-система збирає інформацію про технологічний процес, забезпечує інтерфейс з оператором, зберігає історію процесу і здійснює управління процесом в тому об’ємі, в якому це необхідно.

SCADA-системи з'явилися в результаті вирішення проблем побудови високоефективних і високонадійних систем диспетчерського управління та збору даних. Прообразом сучасних систем SCADA на ранніх стадіях розвитку автоматизованих систем управління були системи телеметрії та сигналізації.

Основна перевага SCADA систем полягає в тому, що вона може надати необхідну інформацію через показники, які зібрані абсолютно з різних точок господарюючого об'єкта в реальному часі. Тільки в такому режимі можна оптимально управляти підприємством, забезпечуючи безперервність його роботи, без простоїв, збоїв і можливих аварійних ситуацій.

1.1.1 Основні функції SCADA систем

SCADA системи повинні забезпечувати виконання наступних основних функцій [1]:

1. обмін даними з «пристроями зв'язку з об'єктом» (тобто з промисловими контролерами і платами вводу-виводу) в реальному часі через драйвери;
2. обробку інформації в режимі реальному часі;
3. логічне управління;
4. відображення інформації на екрані монітора в зручній і зрозумілій для людини формі;
5. ведення бази даних реального часу з технологічною інформацією;
6. аварійну сигналізацію і управління сповіщеннями про аварійні ситуації;
7. підготовки та генерування звітів про хід технологічного процесу;
8. здійснення мережевої взаємодії між SCADA ПК;
9. забезпечення зв'язку з зовнішніми додатками (СУБД, електронні таблиці, текстові процесори і т. д.).

Наведений перелік функцій не є вичерпним і залежить від особливостей системи, які встановлені на конкретному підприємстві.

1.1.2 Основні компоненти SCADA систем

SCADA-система зазвичай містить такі підсистеми [2,3]:

1) драйвери або сервери введення-виведення — програми, що забезпечують зв'язок SCADA з промисловими контролерами, лічильниками, АЦП і іншими пристроями введення-виведення інформації;
2) диспетчерська система (головний термінал) (MTU англ. Master Terminal Unit) — збирає дані про процес і відправляє команди процесору (керування);
3) програмований логічний контролер (PLC англ. Programmable Logic Controller) використовується як польовий пристрій у зв'язку з вищою ніж

у RTU спеціального призначення економічністю, універсальністю і гнучкістю;

4) комунікаційна інфраструктура (CS англ. Communication System) для реалізації промислової мережі;
5) система реального часу — програма, що забезпечує обробку даних в межах заданого тимчасового циклу з урахуванням пріоритетів;
6) людино-машинний інтерфейс (HMI англ. Human Machine Interface) — інструмент, який подає дані про хід процесу людині операторові, що дозволяє операторові контролювати процес і управляти ним;
7) абонентський кінцевий блок (віддалений термінал) (RTU англ. Remote Terminal Unit), що під'єднується до датчиків процесу, перетворює сигнал з датчика в цифровий код і відправляє дані в диспетчерську систему;
8) програма-редактор для розробки людино-машинного інтерфейсу;
9) система логічного управління — програма, що забезпечує виконання призначених для користувача програм (скриптів) логічного управління в SCADA-системі. Набір редакторів для їх розробки;
10) база даних реального часу — програма, що забезпечує збереження історії процесу в режимі реального часу;
11) система управління тривогами — програма, що забезпечує автоматичний контроль технологічних подій, віднесення їх до категорії нормальних, що попереджають або аварійних, а також обробку подій оператором або комп'ютером;
12) генератор звітів — програма, що забезпечує створення призначених для користувача звітів про технологічні події. Набір редакторів для їх розробки;
13) зовнішні інтерфейси — стандартні інтерфейси обміну даними між SCADA та іншими додатками. Зазвичай OPC, DDE, ODBC, DLL і т. д.

Загальна схема АС «SCADA» представлена на рисунку 1.1.

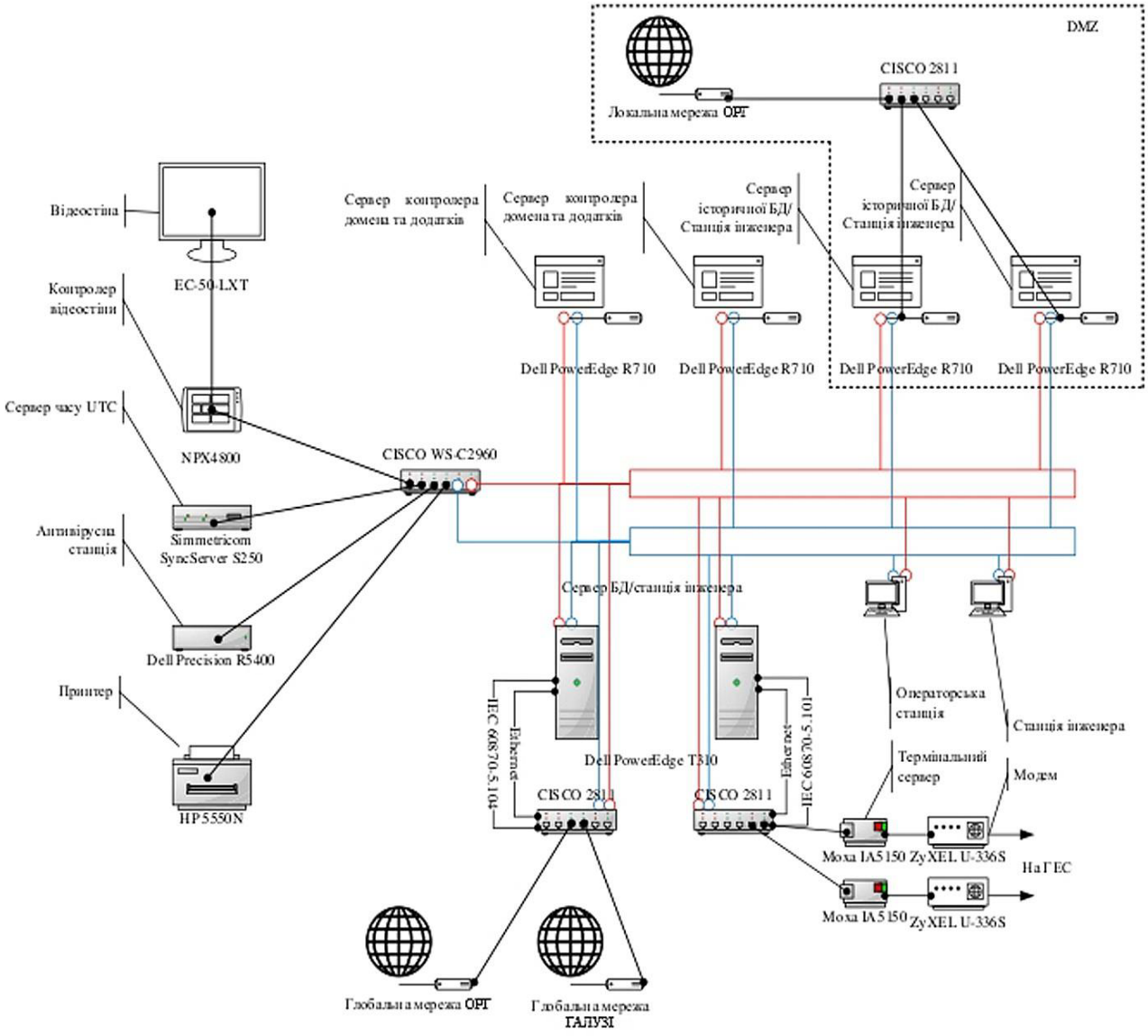


Рисунок 1.1 – Загальна схема АС «SCADA»

1.1.3 Особливості процесу управління в SCADA системах

У систем SCADA обов'язкова наявність людини (оператора, диспетчера).

Будь-яка неправильна дія може призвести до відмови об'єкта управління або навіть катастрофічних наслідків. Диспетчер несе, як правило, спільну відповідальність за управління системою, яка, при нормальних умовах, тільки зрідка вимагає підстроювання параметрів для досягнення оптимального функціонування. Більшу

частину часу диспетчер пасивно спостерігає за інформацією, яка збирається та оброблюється в системі. Активна участь диспетчера в процесі управління відбувається нечасто, зазвичай в разі настання критичних подій - відмов, аварійних і позаштатних ситуацій тощо. Дії оператора в критичних ситуаціях можуть бути жорстко обмежені за часом (декількома хвилинами або навіть секундами).

1.1.4 Архітектура SCADA систем

Як правило, SCADA системи - це двох чи трьох рівневі системи, так як саме на цих рівнях реалізується безпосереднє управління технологічними процесами. Приклад архітектурної реалізації SCADA системи представлено на рисунку 1.2.

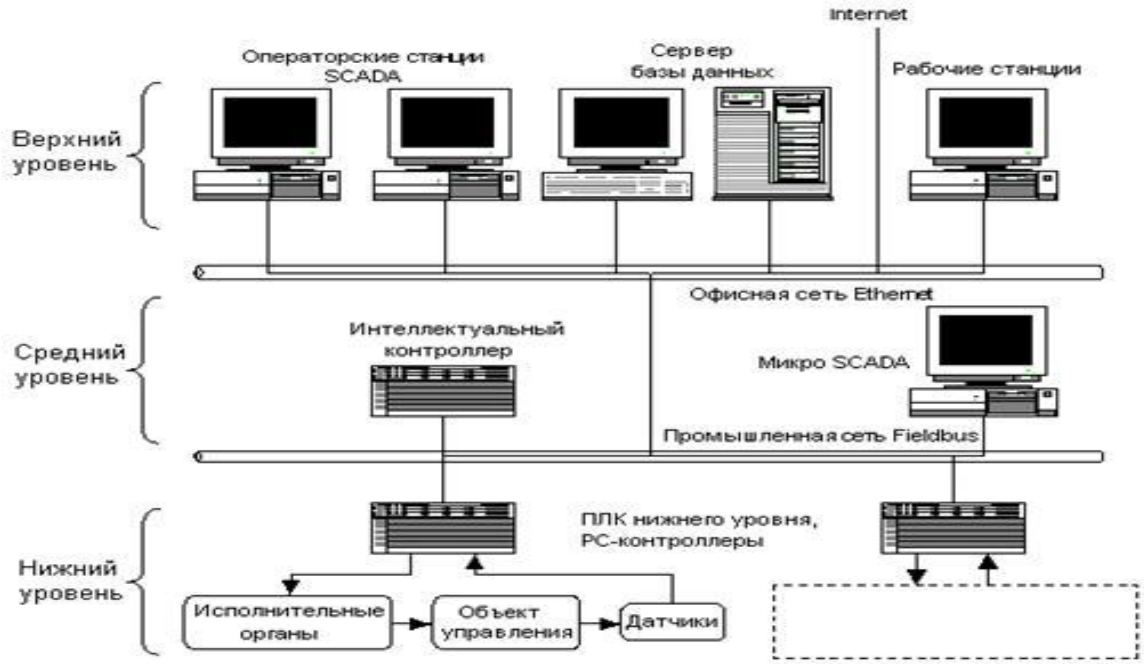


Рисунок 1.2 – Приклад архітектури «SCADA» систем

Нижній рівень - рівень об'єкта включає різні датчики, електроприводи і виконавчі механізми для реалізації регулюючих і керуючих впливів. Датчики поставляють інформацію локальним ПЛК, які виконують такі функції:

- збір і обробка даних про параметри технологічного процесу.
- управління електроприводами і іншими виконавчими механізмами.

- вирішення завдань автоматичного логічного управління і ін.

Так як інформація в контролерах попередньо обробляється і частково використовується на місці, то істотно знижуються вимоги до пропускної здатності мережі.

До апаратно-програмних засобів нижчого рівня управління висуваються жорсткі вимоги щодо надійності, часу реакції на зовнішні події, що надходять від об'єкта.

Для критичних з цієї точки зору об'єктів рекомендується використовувати контролери, що функціонують в режимі жорсткого реального часу. Розробка, налагодження та виконання програм управління контролерами здійснюється за допомогою спеціалізованого ПЗ, наприклад, ISaGRAF.

Середній рівень. Інформація з локальних контролерів направляється в мережу диспетчерського пункту безпосередньо або через контролери верхнього рівня (концентратори, інтелектуальні або комунікаційні контролери) які реалізують такі функції:

- збір і обробка даних з локальних контролерів;
- підтримання єдиного часу в системі і синхронізація роботи підсистем;
- організація архівів за обраними параметрами;
- зв'язок різнорідних мереж і обмін даними між нижнім і верхнім рівнем;
- робота в автономному режимі при порушеннях зв'язку з верхнім рівнем;
- резервування каналів передачі даних і ін.

Верхній рівень. Диспетчерський пункт включає, одну чи кілька станцій управління, що представляють собою автоматизоване робоче місце (АРМ) диспетчера, сервер бази даних, і т. д. Часто в якості робочих станцій використовуються ПК. Станції управління призначені для відображення ходу процесу і оперативного управління. Ці завдання покликані вирішувати SCADA - системи.

1.2 Атаки та вразливості SCADA систем

Останні десятиліття SCADA системи стають привабливою ціллю. За даними аналітиків, спостерігається значний приріст цільових показників на промислових інформаційних системах з метою промислового шпіонажу, шахрайства і порушення функціонування підприємства. Так, наприклад, на зміну окремим «червяками» Stuxnet (2010) і Flame (2012) прийшли набагато серйозніші та складніші схеми багатоступеневих атак. Одним з яскравих прикладів атаки на SCADA систему – це було поширення троянського коня Гавекс в 2014 році. Хакери зламували сайти виробників програмного забезпечення для управління промисловими підприємствами (SCADA) та заражали ним офіційні дистрибутиви SCADA-систем, які потім встановлювались на підприємствах. Дана реалізація атаки дозволила хакерам отримати повний контроль над зараженими системами, що були встановленні на підприємствах в декількох європейських країнах.

Оцінка стану безпеки SCADA систем була проведена в 2012 році компанією «Positive Technologies». В результаті проведення дослідження було отримано доволі тривожну картину. Було виявлено, що з кожним роком різко збільшується кількість виявлених вразливостей. З 2010 по 2012 г. встановлено в 20 разів більше вразливостей, ніж за попередні 5 років. Кожна п’ята вразливість усувається довше місяця. 50% вразливостей дозволяють хакеру запустити код на виконання. Для 35% вразливостей є експлойти. Більше 40% доступних та відкритих в Інтернеті SCADA систем можуть зламати хакери-початківці.

Серед усіх типів уразливих компонентів АСУ ТП лідирують SCADA - 87%, далі йдуть системи, що забезпечують людино-машинні інтерфейси, - 49%, менше виявляються уразливості в програмованих контролерах - 20% і найменше в використовуваних протоколах - 1%.

Найпоширеніші типи вразливостей SCADA-систем [4]:

- вразливості аутентифікації вузлів в результаті «слабких» парольних налаштувань (Authentication). Велика частка таких вразливостей пов'язана з

використанням стандартних інженерних паролів, встановлених виробниками на приладах промислової автоматики. Крім того, користувачі системи часто нехтують безпекою системи та використовують прості паролі, ті, які можна легко запам’ятати або, навпаки, занадто складні для запам'ятовування паролі з подальшим їх відкритим зберіганням. В результаті цього - такі паролі так само можуть бути легко визначені або здобуті з використанням соціальної інженерії;

- уразливості шифрування через використання «слабких» криптографічних алгоритмів і систем управління ключами (Key Management);
- уразливості через помилки конфігурації SCADA-системи (помилки налаштування мережевого обладнання та мережевих служб ОС, помилки при розмежуванні прав доступу і повноважень, помилки при заданні дозволів на доступ до ресурсів, застосування стандартних шаблонів безпеки і т. п.). часто виробник системи встановлює неоптимальні політики безпеки або за замовчуванням встановлює адміністративні права доступу;
- уразливості, викликані відсутністю оновлень безпеки для різних версій SCADA-систем або несвоєчасністю їх установки;
- уразливості програмно-апаратних компонент, що дозволяють використовувати DoS-атаки для автоматичного виконання протоколів аварійних або позаштатних ситуацій, завершення або «зависання» програм, експлуатації в системі шкідливого коду. Як правило, такі уразливості пов'язані з помилками програмістів - виробників SCADA. Помилка в програмі може дозволити зловмиснику використовувати відриті порти для запуску шкідливого коду в системі, проведення DoS-атаки для переповнення розміру буферу даних і т.п.

Розподіл вразливостей SCADA-систем за типами наведено на рисунку 1.3.

Як можна побачити на рисунку, найбільш часто проводяться атаки, що використовують уразливості аутентифікації, і атаки, пов'язані з переповненням буферу програмно-апаратних засобів.

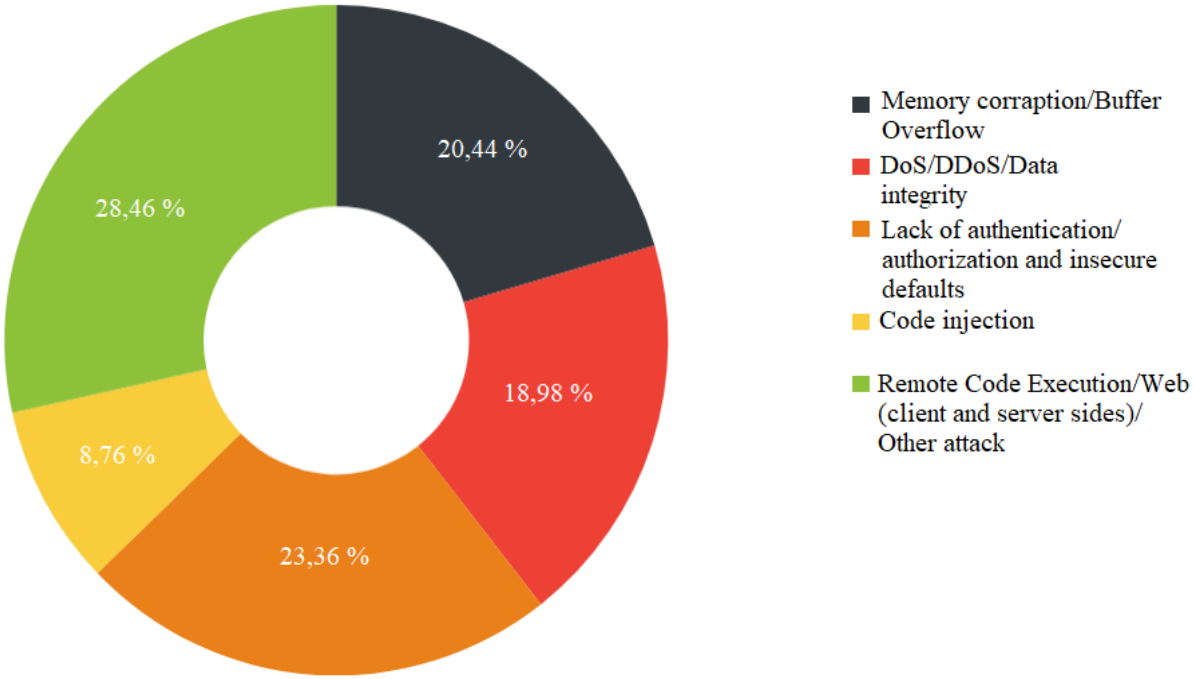


Рисунок 1.3 – Класифікація вразливостей за типами

В області захисту систем управління (ControlSystems, SCADA) на даний момент існує цілий ряд стандартів і рекомендацій, які можна класифікувати наступним чином:

1) галузеві рішення:
   - стандарти NERC для систем управління електричними мережами;
   - стандарти ChemITC для хімічної промисловості;
   - Cisco SAFE for PCN - Стандарти Газпрому.
2) рекомендації загального рівня (стандарти NIST, ISA і ін.):
   - ISA S99 - Комітет суспільства приладобудування, системотехніки і автоматизації (ISA);
   - NIST PCSRF Security Capabilities Profile for Industrial Control Systems;
   - IEC61784-4.

При цьому обов’язкове виконання та дотримання будь-яких вимог до відповідності певним критеріям безпеки, які прописані в стандартах чи документації - для комерційних підприємств не потребується.

Висновки до розділу 1

В даному розділі було розглянуто архітектуру, функції та основні аспекти безпеки SCADA систем. Не зважаючи на те, яку важливу роль вони відіграють в сучасному світі, їх використання без дотримання відповідних вимог безпеки може призвести до небажаних результатів. Зважаючи на це, забезпечення безпеки SCADA систем– одне із головних завдань, яке стоїть перед підприємством, в якому функціонує SCADA система.

Проаналізувавши найпоширеніші атаки на SCADA системи можна зробити висновок, що способів, що призводять до компрометації є дуже багато, і для їх реалізації не потрібно бути хакером. Для того щоб здійснити несанкціонований доступ достатньо мати набір спеціальних інструментів, які визначать слабкі місця системи, а потім такі інструменти, які використають її знайдені недоліки .

Одним із способів захисту від вразливостей, а відповідно й від атак, що основуються на них, є вчасне виявлення та усунення проблем, що пов’язані з безпекою. Тому необхідно використовувати методи/підходи, на основі яких буде перевірятись та оцінюватись стан захищеності SCADA системи. Також, такі перевірки є важливими з точки зору попередження атак на систему при вчасному виявленні та виправлення слабких місця, що наявні в системі.

2 АНАЛІЗ СПОСОБІВ ОЦІНКИ ЗАХИЩЕНОСТІ СИСТЕМ

2.1 Тестування на проникнення

Тестування на проникнення - метод нападу на комп'ютерну систему в надії знайти слабкі місця в її безпеці. Якщо тест успішно отримує доступ - це свідчить про те, що функціональність системи і конфіденційні дані можуть бути скомпрометовані. По суті це метод оцінювання захищеності інформаційних систем та об’єктів від несанкціонованого використання.

Існує певна плутанина щодо відмінності між скануванням вразливостей і тестуванням на проникнення, так як ці дві фрази зазвичай взаємозамінні. Однак, їх значення і наслідки дуже різні. Оцінка вразливості шляхом сканування просто ідентифікує їх наявність та результат такої перевірки записується у звіт. В свою ж чергу тест на проникнення намагається використовувати вразливість, щоб визначити, чи можливий несанкціонований доступ або інша шкідлива активність. Тестування на проникнення, як правило, включає в себе тестування мережі проникнення і тестування безпеки системи.

Переваги : показує реальний ризик наявності вразливостей для системи та характеризує здатність кібер-оборони даної інформаційної системи.

Недоліки : досить ресурсоємне вирішення проблеми.

Тести на проникнення можуть бути автоматизовані за допомогою програмних застосунків, або вони можуть бути виконані вручну.

Основні завдання тестування на проникнення:

1) Виявлення, оцінка та спроба експлуатації всіх можливих вразливостей системи.
2) Опис векторів атаки і оцінка ризиків.
3) Надання рекомендацій щодо поліпшення інформаційної безпеки даної системи.

До основних методів аудиту схожих на дії зловмисника відносяться:

1) Розвідка і збір інформації про систему, що атакується: спеціальні пошукові запити, сканування портів.

2) Виявлення засобів захисту інформаційної системи (IDS, IPS).
3) Сканування інформаційної системи за допомогою відомих утиліт і сканерів.
4) Сканування директорій для пошуку чутливої інформації (файли, бекапи бази даних та інше) також використовуючи спеціальні утиліти.
5) Ручний аналіз вразливостей.

Відомо, що існують різні способи проведення тесту на проникнення, а саме: на основі мети або призначення та наданої інформації.

Раніше було розглянуто, що залежно від мети, яку перед собою ставить тестувальник - це може бути процес оцінки вразливість системи або, безпосередньо, тест на проникнення.

Що стосується кількості і доступу до інформації, то існують такі типи тестування інформаційних систем:

1) Тестування «білої скриньки».
2) Тестування «чорної скриньки».
3) Тестування «сірої скриньки».

Тестування чорної скриньки - тестування, при якому тестувальник має доступ до програми тільки через інтерфейс. Тестувальник дивиться на програму, не маючи при цьому доступу до коду. Але так як він все-таки тестувальник, то перевіряє систему не як користувач, а за допомогою своїх стратегій і методів: або вручну, або за допомогою інструментів тестування.

Мета цього способу тестування в тому, щоб перевірити розбіжність поведінки програми з документацією. Є вимоги в документації, ми бачимо, як працює програма, відповідно перевіряємо, де неточність.

Тестування білої скриньки - тестування, при якому тестувальник має доступ до коду. Його ще називають тестуванням скляної скриньки або тестуванням прозорої скриньки. Крім того, що тестувальник може переглядати код, він ще й сам може писати код, використовуючи бібліотеки існуючого програмного продукту.

Ціль цього виду тестування в тому, щоб перевірити кожну стрічку коду, кожен шлях, кожен оператор, тобто перевірити сам код.

Тестування «сірої скриньки» - це поєднання тестування «чорної» і «білої скриньки». Воно використовується для оцінки системи зі сторони перевірки правильності взаємодії його індивідуальних компонентів.

Тестування «сірий ящик» найбільш підходить для тестування SCADA систем.

Оскільки SCADA системи складаються з різних інфраструктурних елементів, то , як на програмному, так і апаратному рівні, тому відповідно повинна бути перевірка їх взаємодії і функціональності.

Для тестування «сірого ящика» використовуються інструменти, націлені на розуміння властивостей системи та оточення, з яким воно взаємодіє.

2.2 Оцінка захищеності SCADA системи на основі 5 етапів

Даний підхід передбачає перевірку та оцінку захисту SCADA систем на основі 5 етапів [6], таких як:

- Визначення Ступеню Ризику «СР»;
- Проведення експертизи;
- Критичний огляд/Аналіз СР;
- Проведення експлуатації атак;
- Рекомендації на рахунок захисту SCADA системи, що перевірялась.

Визначення Ступеню Ризику «СР». Даний етап є ершим етапом оцінки рівня захищеності системи SCADA. Ступінь ризику перевіряється для наявної або нової системи контролю і управління. Точне визначення оцінки на даному етапі є ключовим, оскільки на основі неї будуть складатись подальші концепції та стратегії захисту системи. Невірна оцінка «СР» може дати обернений ефект і замість того, щоб побудувати на основі отриманої оцінки захищену систему, можна забезпечити додатковий доступ для атак.

Проведення експертизи. Щоб уникнути помилкової оцінки «СР» додатково проводяться періодичні фахової експертизи SCADA системи. Аудит безпеки виконується аналітиками підприємства, на якому функціонує SCADA системи. Вони допомагають проаналізувати SCADA систему на всіх її рівнях, ґрунтуючись на специфікаціях, складових програмних модулів, сполучних протоколів, всередині і між -рівневих каналів зв'язку. Експерти, що спеціалізуються на індустріальних, стратегічних SCADA системах, проводять послідовні перевірки відповідно до кожного з наступних етапів експертизи:

- аналіз і опис будь-яких ризиків для системи безпеки;
- аналіз системного захисту від проникнення;
- інспекція внутрішніх протоколів;
- аналіз топології системи і програмного забезпечення і рекомендації для оптимізації.

Критичний огляд/Аналіз СР включає в себе наступний перелік дій:

- опція динамічного безпечного розширення системи, її аутентифікація і авторизація;
- оцінка прийнятих до уваги ризиків;
- аналіз архітектури системної безпеки («АСБ»);
- аналіз існуючого парольного захисту і рекомендації;
- аналіз вимог і можливостей «АСБ» відповідати цим вимогам.

Проведення експлуатації атак. Даний етап включає в себе виконання наступних задач:

- тестування системи на уразливість через авторизований доступ до ресурсів;
- виявлення вразливостей без будь-якої шкоди або небезпеки для критичних систем, які підлягають тестуванню.

Рекомендації із захисту. Даний етап є заключним та в результаті його винання формуються наступні артефакти:

- Рішення і рекомендації для зміцнення захисту системи;

- Рекомендації для перевірених технічних рішень;
- Рекомендації для інтеграції нових технологій з існуючими модулями SCADA системи.

2.3 Формальна модель оцінки захищеності АСУ ТП

В основі даної моделі лежить аналіз загроз на систему SCADA [7].

Спочатку вводиться три множини:

- $X = \{x_j\}$ - множина джерел загроз;
- $T = \{t_i\}$ - множина загроз безпеки;
- M = {mk} - множина механізмів захисту, реалізованих і рекомендованих до впровадження.

Об’єктом оцінки є АСУ ТП .

Захищеність АСУ ТП від загроз безпеки S визначається кількістю вразливостей v, для яких в системі не створено бар'єрів b, що перекривають ці уразливості, а також міцністю існуючих бар'єрів.

В ідеалі кожен механізм захисту повинен виключати відповідний шлях реалізації загрози t_i. Насправді ж механізми захисту забезпечують лише деяку ступінь опору загрозам безпеки. У зв'язку з цим в якості характеристик елемента набору бар'єрів $b_l = <x_j, t_i, m_k>$, може розглядатися набір $<p_k, l_k, r_k>$, де

- P_k - ймовірність появи загрози, яка задається експертним методом;
- L_k - величина збитку при вдалому здійсненні загрози, яка задається експертним методом;
- R_k - ступінь опірності механізму захисту m_k, що характеризується ймовірністю його подолання, яка задається експертним методом.

Міцність бар'єру $b_l = <x_j, t_i, m_k>$ характеризується величиною залишкового ризику $Risk_i$, пов'язаного з можливістю створення іншої загрози безпеки t_i щодо об'єкта АСУ ТП, при використанні механізму захисту m_k. Ця величина визначається за формулою:

$$Risk_i = P_k * L_k (1 - R_k) \quad (2.1)$$

Для визначення кількісного значення оцінки захищеності S можна використовувати наступну формулу:

$$S = \frac{1}{\sum(P_k * L_k\,(1 - R_k))} \tag{2.2}$$

де n - число загроз, P_k, L_k, $R_k \in (0, 1)$.

У цій формулі знаменник визначає сумарну величину залишкових ризиків, пов'язаних з можливістю здійснення загроз безпеки T щодо об'єкта АСУ ТП, при використанні механізмів захисту M.

Сумарна величина залишкових ризиків характеризує «загальну вразливість» системи захисту, а захищеність АСУ ТП визначається як величина, зворотна її «уразливості». При відсутності в системі бар'єрів b_k, що перекривають певні уразливості, ступінь опірності механізму захисту R_k приймається рівною 0.

Висновки до розділу 2

В даному розділі висвітлено та проаналізовано основні способи оцінки захищеності інформаційних систем, в тому числі й SCADA.

Дослідження показало, що кожен із способів виділяє певну групу проблем та направлений на конкретний аспект безпеки SCADA систем.

З цього можна зробити висновок, що не зважаючи на ряд переваг даних способів, окремо кожен з них не здатний забезпечити цілісну перевірку та оцінку захищеності SCADA систем. Також можна побачити, що дані способи перевірки захищеності перетинаються між собою, тобто підходи, що вони використовують не є унікальними для кожного з них. Тому, доцільно було б створити нову модель, яка буде направлена на отримання максимально широкої оцінки захищеності SCADA систем.

3 ПІДХІД ДО ОЦІНКИ ЗАХИЩЕНОСТІ SCADA СИСТЕМ

Безпека SCADA систем включає в себе різноманітні аспекти. Одним із найбільш актуальних є перевірка рівня захищеності. Відомо, що є різні способи оцінки захищеності SCADA систем, проте зазвичай вони не забезпечують комплексну перевірку та оцінку систем. Зважаючи на те, що впровадження цифрових технологій у технологічних галузях створює нові загрози кібербезпеки, які можуть призвести до небажаних аварій SCADA систем, то аналіз цих загроз під час аналізу ризиків стає важливою складовою для ефективної оцінки ризиків. Однак сьогодні поняття ‘safety’ та ‘security’ SCADA системи оцінюються окремо, в той час, коли вони повинні оцінюватись як складові однієї оцінки.

Відмінності та подібності між параметрами ‘safety’ та ‘security’ SCADA системи вивчаються багатьма сучасними науковцями. Загалом, поняття ‘safety’ пов'язане з випадковими ризиками, спричиненими порушенням працездатності компонентів системи, людськими помилками або будь-яким неналежним дотриманням норм безпеки людьми, які працюють з SCADA системою. В той час як поняття ‘security’ пов'язане з навмисними ризиками, що виникають внаслідок реалізації шкідливих атак на SCADA систему. Такі атаки можуть бути здійснені фізично або за допомогою спеціальних кіберзасобів (програмних, програмно-апаратних засобів або інших технічних та технологічних засобів і обладнання). Крім того, причини порушення інформаційної безпеки SCADA системи, пов'язаних з параметром ‘safety’ є внутрішніми і розглядаються як події з трохи меншою ймовірністю, а ніж порушення інформаційної безпеки системи, пов’язане з порушенням ‘security’. Причини аварій пов’язаних з поняттям ‘security’ можуть бути внутрішніми або зовнішніми (напади через посередників або аутсайдерів) і класифікуються як спроби реалізації загально відомих атак.

Основною проблемою існуючих SCADA систем є те, що вони розроблені таким чином, щоб бути надійними, проте не кіберзахищеними.

3.1 Основні етапи підходу до оцінки захищеності SCADA систем

У даному розділі запропоновано новий підхід, в якому оцінка захищеності розраховується через оцінку ризику. Проте, варто зважати, що під час аналізу ризику розглядається 2 типи ризиків, а саме ризиків, пов'язаних з параметрами 'security' і 'safety' SCADA систем разом. Цей підхід також передбачає аналіз сценаріїв порушення безпеки, який зазвичай використовується для аналізу подій, що призводять до порушення безпеки SCADA системи як зі сторони 'safety' так і з сторони 'security'.

Загальна оцінка з точки зору обох параметрів 'safety' і 'security' SCADA системи забезпечує вичерпну оцінку ризику за рахунок аналізу різних сценаріїв ризиків направлених на параметри 'safety' і 'security'. Також основним елементом оцінки є застосування функції правдоподібності при розрахунку загального ризику.

Важливим для розуміння є також той факт, що зібрані з 'safety' події та пов'язані з 'security' події або два цих типи подій разом - можуть стати об'єктом для оцінки безпеки з метою забезпечення повного моделювання сценаріїв ризику. Сценарій ризику буде представляти собою співвідношення всіх очікуваних подій 'safety' і 'security', які можуть привести до небажаних наслідків.

Оцінка захищеності SCADA систем здійснюватися на основі отриманих результатів на 4 нижчевказаних етапах:

1. визначення сценаріїв ризиків;
2. оцінка функції правдоподібності;
3. оцінка збитків, отриманий в наслідок реалізації небажаних сценарії/атак;
4. розрахунок ризику, отриманого в результаті реалізації сценаріїв небажаних подій, пов'язаних з 'safety' та 'security'.

Кожен з цих етапів можна умовно розбити на десятки дій, які повторюються. Якщо умовно згрупувати та об'єднати дії, які повторюються на кожному із етапів, то отримуємо загальний алгоритм, який охоплює всі проміжні етапи при та описує загальний підхід при визначенні оцінки захищеності SCADA системи.

На першому кроці необхідно проаналізувати систему SCADA відносно 7 областей з точки зору ‘safety’ і визначити сценарії ризиків, які пов’язані з ‘safety’ (сценарії відомих атак, які можуть призвести до порушення інформаційної безпеки системи). Будь-який сценарій має включати в себе причину наявності вразливості та наслідок, який буде отримано в результаті реалізації сценарію. Унікальний сценарій характеризується набором параметрів, який повинен містити 2 параметри: причину та наслідок реалізації сценарію. Мінімальний сценарій складається лише з однієї ланки (наприклад, в наслідок відсутності належної організації фізичного доступу, будь яка людина може отримати прямий доступ до SCADA системи та вивести її з ладу в результаті чого підприємство буде простоювати протягом 2 годин). Проте, можуть бути сценарії, які поєднують в собі декілька подій, послідовність яких приведе до досягнення однієї цілі (наприклад, в наслідок відсутності фільтрації вхідних параметрів на рівні БД може бути реалізована атака SQL injection та зловмисник може отримати необмежені права в БД SCADA системи. В результаті чого підприємство буде простоювати протягом 5 годин).

Чим більше уточнюючих моментів визначено в сценарії – тим точніша буде отримана оцінка ризику, отриманого від реалізації небажаного сценарію подій та, відповідно, оцінка захищеності системи вцілому.

Після того, як сценарії порушення безпеки SCADA системи складені, необхідно визначити функцію правдоподібності для цих сценаріїв та оцінити збитки, які будуть в наслідок реалізації сценарію. Зважаючи на відмінності в природі між подіями, пов'язаними ‘security’ та ‘safety’, вони будуть охарактеризовані окремо при оцінці функції правдоподібності.

На рисунку 3.1 зображено деталізований алгоритм оцінки ризиків, який відображає зв’язок та оцінку ризиків пов’язаних з ‘safety’ та ‘security’ системи SCADA на усіх чотирьох кроках.

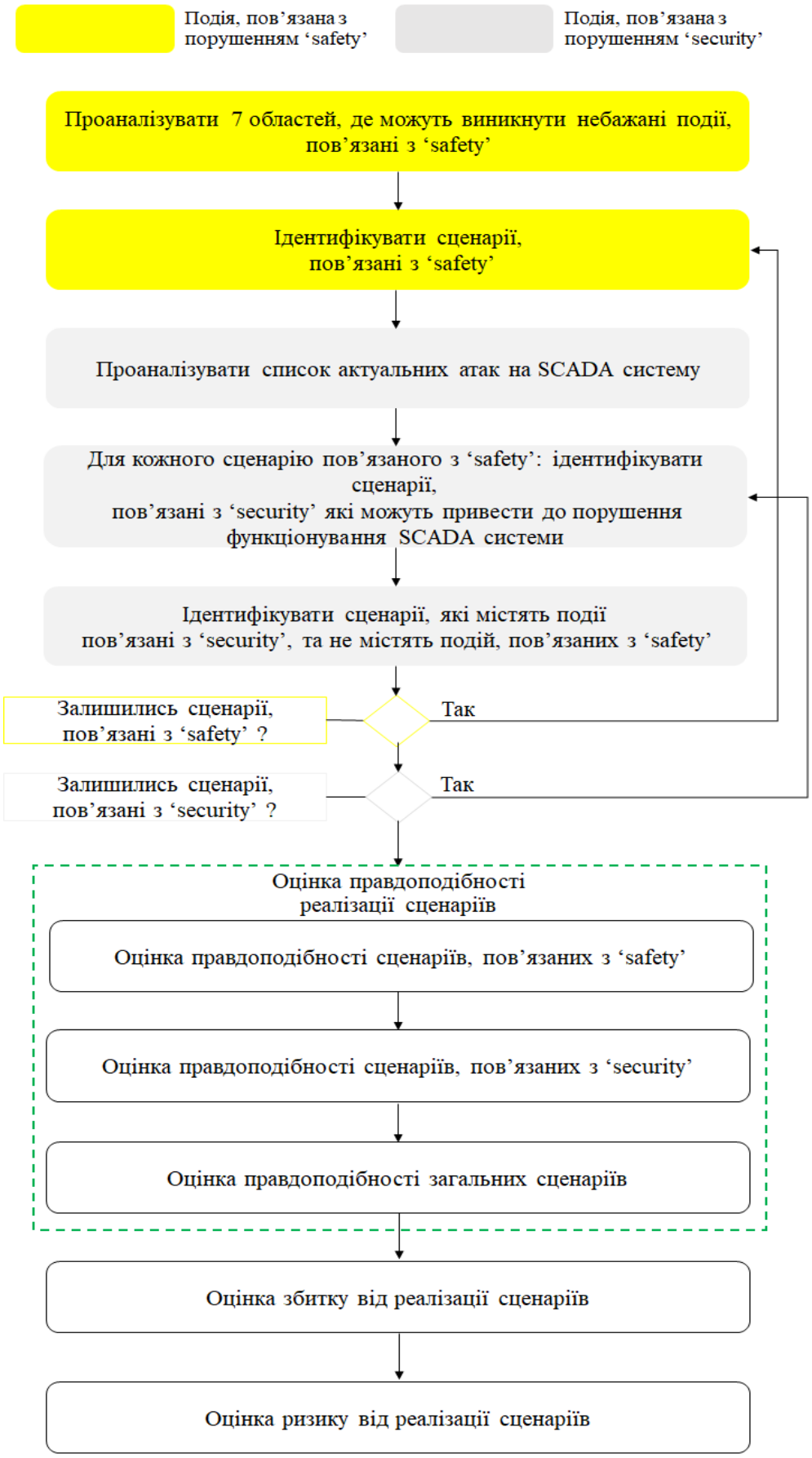


Рисунок 3.1 – Етапи оцінки захищеності

3.1.1 Визначення сценаріїв ризиків

При складанні сценаріїв ризиків буде використовуватись аналіз, який дозволяє описати причини виникнення та наслідки небажаних подій, пов’язаних з ‘safety’ SCADA системи. До кожного такого розробленого сценарію будуть описані атаки, які що можуть бути реалізовані в системі SCADA на основі відомих вразливостей. Атаки на систему та небажані ‘safety’ події можуть аналізувати як разом так і окремо. В залежності від того, чи необхідні ці 2 елементи для досягнення кінцевої цілі, порушення безпеки системи SCADA, чи відразу можна досягнуть бажаної цілі за допомогою реалізації однієї/одного атаки/небажаного сценарію.

Сценарії небажаних подій пов’язані з ‘safety’ системи SCADA можуть виникати в результаті недотримання/не виконання вимог безпеки в наступних 7 областях:

- фізична безпека SCADA систем:
  - організація фізичного доступу до SCADA систем;
  - безпека розміщення і обслуговування SCADA системи на підприємстві;
  - безпека переміщення та знищення елементів SCADA систем чи самої системи на підприємстві.
- неперервність роботи SCADA систем:
  - план відновлення роботоздатності SCADA системи в разі виникнення аварійної ситуації;
  - перелік відповідальних працівників за процес відновлення роботоздатності SCADA;
  - ролі та відповідальності в процесі відновлення роботоздатності SCADA.
- резервне копіювання SCADA системи:
  - план резервного копіювання;
  - місця збереження резервних копій;
  - відновлення даних з резервних копій.

- логічний доступ до SCADA систем:
  - організація видачі прав доступу до системи SCADA на підприємстві.
  - організація видачі адміністративних прав доступу до системи SCADA на підприємстві.
  - організація віддаленого доступу до системи SCADA.
- налаштування безпеки на інфраструктурних рівнях таких як:
  - операційна система;
  - база даних;
  - застосунок.
- управління інцидентами:
  - процедура реагування на інциденти;
  - сроки реагування на інциденти;
  - розробка та впровадження превентивних мір для попередження аналогічних інцидентів.
- логування дій користувачів в системі SCADA
  - налаштування процедури логування дій;
  - сбір логів та переміщення їх в окремі місця зберігання;
  - доступ до логів з діями користувачів;
  - архівація та знищення логів.

Наприклад, можна ідентифікувати наступні сценарії небажаних подій пов’язані з ‘safety’ системи SCADA:

- відсутність періодичного резервного копіювання може привести до втрати усіх конфіденційних даних, які зберігались у SCADA системі;
- не виконання умов обслуговування SCADA системи третіми особами може привести до отримання неавторизованого доступу до SCADA системи сторонніми особами;
- компрометація системи контролю доступу до приміщення, в якому розташовані сервери SCADA системи, може привести до несанкціонованому доступу персоналу до заборонених зон;

- відсутність плану відновлення роботоздатності SCADA системи в разі виникнення аварійної ситуації може привести до простою системи більше ніж на 8 годин, що є дуже критичним;
- відсутність стійких парольних налаштувань може привести до компрометації облікового запису працівника та отримання неавторизованого доступу до SCADA системи;
- відсутність чітких сроків реагування на інциденти може привести до невчасного виявлення вирішення інцидентів та втрати важливих даних, які зберігаються в SCADA системі чи до отримання неавторизованого повного доступу на рівні SCADA систем;
- відсутність обмеженого доступу до логів системи з діями користувачів може стати причиною приховання неправомірних дій зі сторони Адміністраторів SCADA системи.

Як було вказано раніше, ці небажані ‘safety’ події можуть статись в результаті неправильного забезпечення рівні безпеки зі сторони працівників підприємства, в якому функціонує SCADA система.

Щодо сценаріїв атак, які пов’язані з ‘security’, то тут є певні особливості. Атак на систему SCADA є багато, оскільки системи SCADA можуть різнитись за параметрами такими як:

- виробник;
- країна, де обслуговується система (зважаючи на вимоги законодавства різних країни - функціонал системи одного виробника може різнитись та нові доопрацювання системи можуть бути здійснені в рамках замовлення самого підприємства, на якому обслуговується система);
- версійність систем.

На основі аналізу вразливостей систем SCADA та існуючих атак [6,8], які направлені на даний тип систем, було виділено 9 атак, які є загальними для всіх типів SCADA систем. Вони є найнебезпечнішими з точки зору того, що вони є най-

частішими та стабільними за останні 8 років. За цей проміжок часу, лише змінюється кількість та частота виникнення атак того чи іншого роду. Як було доведено Positive Technologies [6], SCADA є найбільш чутливою та цілеспрямованою частиною промислової автоматизації з точки зору кібербезпеки.

Оскільки будь-яке складне середовище SCADA можна звести до найпростіших компонентів, які з'єднуються через протоколи зв'язку, то нижче в даній роботі будуть представлені атаки, які направлені на кожен з цих компонентів. Дана архітектура зображена на рисунку 3.2

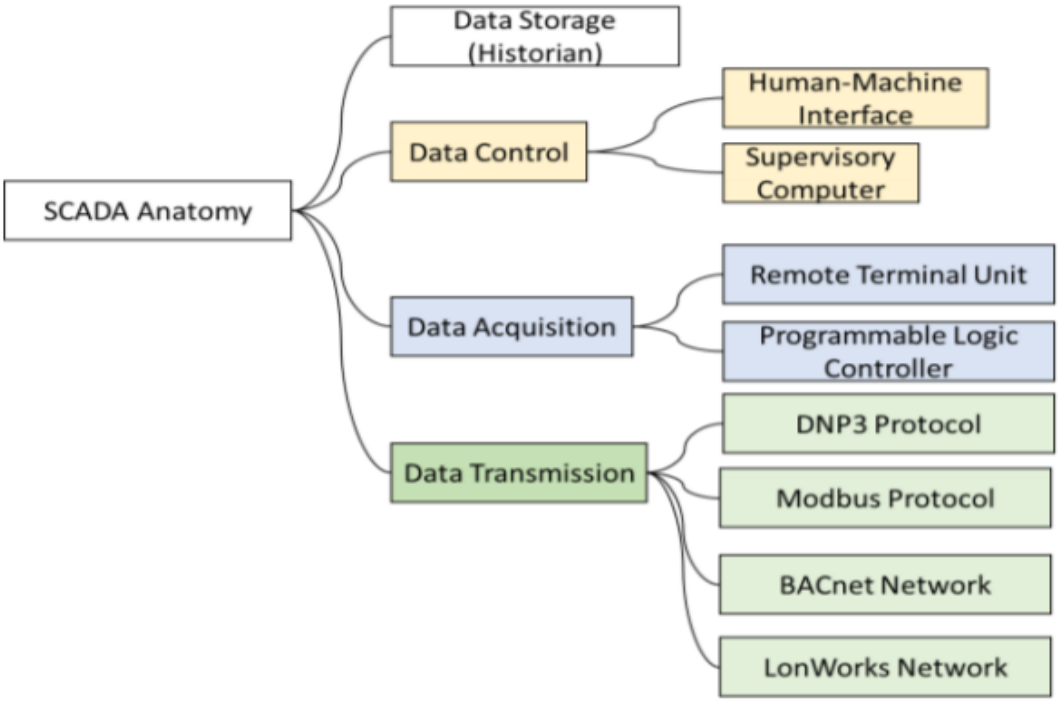


Рисунок 3.2 – Архітектура основних компонентів SCADA системи

1. першим компонентом – є місце зберігання даних (Data storage). В межах мережі SCADA зберігання даних необхідне для майбутньої або постійної аналітики. Дані, отримані з мережі SCADA, використовуються для корегування поточних процесів і розшифровки, якщо поточний процес знаходиться в межах специфікації. Historian data - це програмне забезпечення,

яке може працювати на контрольованому комп'ютері або на спеціалізованій машині. Historian - це системи баз даних, які зберігають дані реального часу з мережі SCADA. Зважаючи на те, безпека даних є основною проблемою в системах SCADA, відповідно на це направлено і найбільше атак. В результаті аналізу було виділено наступні атаки на місце зберігання даних:

- переповнення буфера (Buffer Overflow): Historian системи піддаються ризику помилки переповнення буфера. Було помічено, що даний компонент SCADA системи може бути віддалено атакований через TCP порт 777, що в свою чергу викликає переповнення буфера;
- SQL-ін’єкції (SQL Injection): оскільки основний інфраструктурний компонент місця зберігання даних - це бази даних, які відповідно мають зручний веб-інтерфейс як для адміністрування, так для використання. Використовуючи веб-інтерфейс, зловмисники можуть експлуатуватимуть різні форми для введення даних, які представленні як частина інтерфейсу (наприклад, форму авторизації/автентифікації) для виконання несанкціонованих запитів, використовуючи структуровану мову запитів (SQL). В результаті успішного виконання, атака може завдати шкоди даному компоненту SCADA системи або системі в цілому;
- міжсайтові сценарії (Cross-Site Scripting): як вже було сказано вище, багато Historian зараз використовують певний веб-інтерфейс. Або для віддаленого адміністрування, або для системного інтерфейсу користувача. Ці форми схильні не лише до SQL-ін’єкцій, а й до вразливостей веб-сторінок. Одна із причин вразливості - відсутність серверної перевірки вхідних параметрів. Ця атака є небезпечною та може бути віддалено експлуатована на SCADA системи тих організацій, які дозволяють веб-інтерфейсу бути зовні;

- порушення пам'яті (Memory corruption): це атака, яка може бути виконана внутрішньо або віддалено в залежності від доступу до місця зберігання даних. У 2012 році після масової реалізації даного типу атаки було виявлено, що сховища даних були віддалено атаковані через TCP порт 14000, що в свою чергу привело до порушення сховища. Також, дана атака може призвести до віддаленого виконання коду та втрати даних та втрати даних. Наведений приклад, є одним із сценаріїв, пов’язаних з ‘security’, проте він не єдиний;
- відмова в обслуговуванні (DoS): однією із причин виникнення уразливості DoS на сховище даних є використання додаткового елементу керування ActiveX. Для проведення даної атаки, необхідно щоб сховище даних взаємодіяло з програмним забезпеченням ActiveX. Тобто основний вектор атаки направлений на вразливості програмне забезпечення ActiveX за допомогою якого можна отримати повний доступ до сховища даних;
- обхід каталогів: однією із причин даної атаки є розміщення файлів, директорій і команд поза межами основної директорії веб-сервера. Зловмисник може маніпулювати параметрами URL, щоб отримати доступ до файлів або виконати команди, які можуть бути розміщені у файловій системі. В результаті успішної реалізації атаки отримати несанкціонований доступ до мережі і відкрито читати файли через HTTP-запити без попередньої аутентифікації або соціальної інженерії.

2. другим компонентом – є контролер даних (Data control). Для управління даними SCADA збирає та передає команди керування до підключених пристроїв. Системи SCADA використовують контрольні комп'ютери, які встановлені з унікальним інтерфейсом людина-машина (HMI), щоб відповідати за комунікацію з контролерами підключення (тобто віддаленими термінальними блоками (RTU) і програмованою логікою контро-

лерів (PLC)) і включають програмне забезпечення HMI, що працює на робочих станціях оператора. Керування даними є критичним компонентом SCADA. Зважаючи, що є 2 контролери даних – то було виділено 2 блоки атак, окремо на контролюючий комп’ютер (2 атаки) та на людино-машину (6 атак):

- фізичні атаки: основною причиною фізичних атак на контрольні комп'ютери є людські помилки. На відміну від інших атак, фізичні атаки зазвичай трапляються, коли працівники ігнорують практику безпеки, в наслідок чого зловмисники отримують прямий доступ до контролюючого комп’ютера;
- відмова в обслуговуванні (DoS): це одна з найбільш поширених атак на контролюючі комп'ютери, тому є декілька сценарії небажаних подій, пов’язаних з даним типом атак. Одними із основних причин є застаріле ПО (наприклад, операційна система), контрольні комп'ютери чи мережа, до якої вони підключені можуть бути недоступними для користувачів, що в результаті викликає тимчасову відсутність або невизначеність в наданні послуг і простій системи. Також причинами може бути відсутність фільтрації трафіку та засобів реагування, таких як IPS система;
- пошкодження пам'яті (Memory corruption): пошкодження пам'яті відбувається в HMI, коли вміст пам'яті ненавмисно змінюється через помилки програмування, що викликають порушення безпеки пам'яті. MICROSYS PROMOTIC є прикладом вразливості до пошкодження пам'яті. MICROSYS PROMOTIC - це набір програмного забезпечення для програмного забезпечення SCADA HMI на базі Microsoft Windows.
- переповнення буфера: причиною переповнення буфера на HMI є спеціально розроблений пакет, який надсилається службі прослухову-

вання HMI PLC, який запускає віддалено необхідний буфер для переповнення. Також ця вразливість відома як UCanCode, оскільки впливає на одну з функцій UCanCode. В результаті вдалого виконання атаки зловмисник має змогу завантажити і виконати довільний машинний код від імені програми і з правами облікового запису, від якої вона виконується

- захоплення облікового запису: причиною втрати HMI своєї функціональність є встановлення параметрів системи за замовчуванням (парольні налаштування). І під час передачі даних в режимі реального часу для створення графіків - конфіденційні дані, зібрані HMI, можуть бути викрадені та розголошені;
- SQL ін'єкція (SQL Injection) – причиною даної атаки є наявність вебінтерфейсу з формами для введення даних, які представленні як частина інтерфейсу (наприклад, форма авторизації/автентифікації), яку зловмисники використовують для виконання несанкціонованих запитів, з допомогою структурованої мови запитів (SQL). В результаті успішної експлуатації атаки ін'єкції коду зловмисник матиме змогу підміняти ідентичність, втручатися в існуючі дані, зібрані HMI, викликаючи проблеми відмови, такі як анулювання транзакцій або повне розкриття всіх даних системи, включаючи конфіденційні дані;
- виконання неавторизованого коду: існує багато рівнів контролю доступу, які операційна система надає користувачам, щоб захистити системні файли та функції від випадкового чи навмисного зміни. Системний рівень дозволяє будь-якій особі запускати програми з правами адміністратора. Це може бути дуже небезпечно, якщо HMI працює на системному рівні. Оскільки, це може стати тунелем відправки шкідливого програмного забезпечення до системи, який буде керуватися хакерами з правами адміністратора. Наявність даної вразливості дозволяє авторизованому користувачеві системи змінювати конфігурацію

служби CIMPLICITY GE Proficy HMI SCADA і запускати будь-який виконуваний файл в системі як службу.

3. третім компонентом – є процеси збору даних (Data Acquisition). Збір даних у середовищі SCADA - це процеси збору інформації призначені також для документування або аналізу деяких явищ. Збір даних починається на рівні RTU або PLC, що включає показання параметрів датчиками, які передаються в систему SCADA. Часті атаки на пристрої збору даних, такі як RTU і PLC, роблять його одним з важливих пристроїв для захисту в системах SCADA. Нижче описані атаки, побудовані на використанні як RTU (6 атак), так і PLC (5 атак):
    - модифікація повідомлень: якщо RTU підтримує незахищений протокол SCADA, який може бути прямо атакований і використаний для керування або пошкодження підключених об'єктів. Надсилаючи спеціально створені неправильні повідомлення RTU для підключених об’єктів може відбутися переповнення буфера, що призводить до відмови в обслуговуванні (DoS);
    - спуфінг (Spoofing): неправильне використання криптографії може привести до появи для зловмисників можливості віддалено підміняти потік даних контролера до бази;
    - сніфінг (Sniffing): відсутність механізму аутентифікації дає змогу зловмиснику читати всі види інформації RTU (наприклад, статус, розташування, тип програмного забезпечення, тощо), а також пристроїв SCADA (таких як датчики, приводи);
    - інсайдерські атаки: незадоволені інсайдери можуть стати головним джерелом комп'ютерних злочинів, оскільки вони знають і мають доступ до внутрішніх систем. Інсайдери включають співробітників, ділових партнерів та постачальників. Інсайдери не обов'язково можуть бути шкідливими, але випадкові помилки можуть мати такі ж нас-

лідки, як шкідливі атаки. Наприклад, інсайдер може бути нічним охонцем, який використовувати свою позицію щоб отримати фізичний доступ до систем управління і маніпулювати цими системами;

- переповнення буфера на основі стека: на основі уразливості протоколу Modbus, яка дозволяє зловмиснику виконувати атаки переповнення буфера на основі стека, які, у свою чергу, надають атакуючому контроль над будь-яким PLC;
- ескалація привілеїв: основою даної атаки є те, що спочатку зловмисник отримує певний рівень доступу, який зазвичай є рівнем доступу користувача, а потім намагається збільшити отримані права, змінюючи конфігурації контролю доступу. В результаті реалізації даної атаки, будь-який зловмисник, який використовує цю вразливість, може вимкнути пристрій, скомпрометувати цілісність пристрою та віддалено виконати код на цільовій системі;
- атаки на операційну систему: кожен контролер RTU або PLC на ринку має комерційну операційну систему (наприклад, Microware OS-9, VxWorks тощо). Причиною реалізації даної атаки є наявність вразливих місць, які можу бути використані для впровадження шкідливих програм (наприклад, черв'яків, вірусів та троянських коней). Це може привести до втрати конфіденційних даних або спотворення даних, які передаються в режимі реального часу;
- модифікація логіки трапу (Modifying Ladder Logic): ladder logic є методом документування проектування та будівництва релейних стійок, які використовуються у виробництві та керуванні технологічними процесами. Логічний трап використовується для розробки PLC, який в свою чергу використовуються в промислових приладах керування. Отримавши привілей для атаки Ladder Logic, зловмисник може змінювати логічну логіку (програми PLC) і впливати на функціональність

програми. Використання вразливості може дозволити будь-якому користувачеві мережі взаємодіяти з керуванням процесом і змінити логічну схему;

- підробку запитів між сайтами (CSRF): дана атака може бути реалізована у випадку, коли зловмисник змушує автентифікованого користувача виконувати авторизовану команду на веб-застосунку. В результаті виконання такої атаки зловмисник може скомпрометувати цілісність та доступність пристрою PLC;
- захоплення веб-сесії (Hijacking Web Session): причною даної атаки може бути відсутність ентропії при генерації випадкового числа, в результаті чого зловмисник може захопити веб-сесію PLC без аутентифікації. В свою чергу викрадення веб-сесії може спричинити крадіжку або модифікацію даних.

4. четвертою складовою є передача даних: протоколи і мережі (Data Transmissions: Protocols and Networks). Процеси передачі даних є особливо вразливими до атак sniffing та модифікації даних. Найпоширеніший розподілений мережевий протокол DNP3 використовується у середовищі автоматизація SCADA систем. Через його широке використання і притаманний слабкий механізм безпеки, даний протокол часто стає мішенню зловмисників. Як протокол DNP3, Modbus протокол також широко використовується в промисловій автоматизації і використовується для послідовного зв'язку між компонентами SCADA, наприклад, зв'язку між пристроями RTU з сховищем даних. В основному, відсутність механізму аутентифікації та авторизації робить цей протокол вразливим для атак. Нижче описані найпростіші сценарії, пов’язані з ‘security’ на основі атак на DNP3 і протокол Modbus:
   - атака DDOS: причиною реалізації розподілених атак відмови в обслуговуванні (DDoS) є відсутність властивостей безпеки аутентифікації в

протоколі DNP3. Дана атака може привести до втрати даних чи втрати функціональності системою;

- атака «Людина по середині» (Man in the Middle Attack): причиною даної атаки є слабке шифрування протоколу DNP3, в наслідок чого людина посередині може перехопити з'єднання, розмістивши себе посередині з'єднання між відправником і приймачем та отримати доступ до конфіденційної інформації;
- виконання несанкціонованих команд: причиною даної атаки є відсутність аутентифікації в протоколі Modbus, в наслідок чого можна надіслати підроблене повідомлення для виконання довільної несанкціонованої команди та отримати неавторизований доступ до SCADA систем;
- переповнення буфера на основі стека: Причиною даної атаки є наявність вразливості в протоклі Modbus, що дозволяє зловмиснику виконати атаки на переповнення буфера, які, у свою чергу, приводять до можливості управління будь-яким PLC зловмисником.

Отже, атаки направлені на порушення параметру ‘security’ різних складових системи SCADA є схожими та навіть в деякій мірі перетинаються. Провівши аналіз та виділивши основні типи атак, які направлені на ‘security’ системи SCADA було сформовано наступний список основних атак:

1. Переповнення буферу (Buffer Overflow);
2. Атака відмови в обслуговуванні (DoS);
3. Пошкодження пам’яті (Memory Corruption);
4. Модифікація повідомлень (message modification);
5. Модифікація логіки трапу (modifying ladder logic programs);
6. Атака відмови в обслуговуванні (DDOS);
7. Неавторизоване виконання команд (Unauthorized Command Execution);
8. Спуфінг (Spoofing);
9. Атака підбору паролів (Brute-force attacks).

Даний список може бути розширений чи доповнений за необхідністю. Оскільки це мінімальний набір атак, на стійкість до яких має бути перевірена система SCADA.

В таблиці 3.1 представлено основні вразливості, на основі яких дані атаки реалізовуються, спосіб реалізації та походження атаки (локально чи віддалено вона реалізується). Дана інформація може бути основою при розробці та аналізі сценаріїв небажаних подій, пов’язаних з ‘security’ SCADA системи.

Таблиця 3.1 - Базова інформація для формування сценаріїв

Назва атаки	**Вразливість, яка використовується**	**Спосіб реалізації**	**Походження атаки**
Переповнення буферу (Buffer Overflow)	Немає чітко визначених меж буферу	Компроментація зі сторони користувача/шкідливі програми	Віддалена атака
Атака відмови в обслуговуванні (DoS)	Застаріле ПО (наприклад, операційна система)	Компроментація зі сторони користувача/шкідливі програми	Віддалена атака
Пошкодження пам’яті (Memory Corruption)	Відсутність перевірок меж пам’яті	Компроментація зі сторони користувача/шкідливі програми	Локальна атака
Модифікація повідомлень (message modification)	Вразливості в програмному забезпеченні	Шкідливі програми/віруси	Віддалена/локальна атака

Продовження таблиці 3.1

Модифікація логіки трапу (modifying ladder logic programs)	Наявність бекдорів	Шкідливі програми	Локальна атака
Атака відмови в обслуговуванні (DDOS)	Відсутність авторизації	Компроментація зі сторони користувача/шкідливі програми	Віддалена атака
Неавторизоване виконання команд (Unauthorized Command Execution)	Відсуність аутентифікації	Шкідливі програми	Віддалена атака
Спуфінг (Spoofing)	Відсуність аутентифікації	Компроментація зі сторони користувача	Локальна атака
Атака підбору паролів (Brute-force attacks)	Слабкі парольні конфігурації	Компроментація зі сторони користувача/шкідливі програми	Віддалена атака

Отже, є атаки, які можуть бути основою мінімального сценарію, тобто не потребується додаткових небажаних подій, які пов’язані з ‘safety’ щоб досягнути поставленої мети зловмиснику, оскільки слабкі місця вже закладені в програмному забезпеченні чи протоколах. Проте, існують сценарії, які все ж таким можуть бути комбінацією небажаних подій, пов’язаних з ‘safety’ та ‘security’, які в поєднанні призводять до компрометації системи чи компонентів системи. Схематично, такий сценарій представлено на рисунку 3.3.

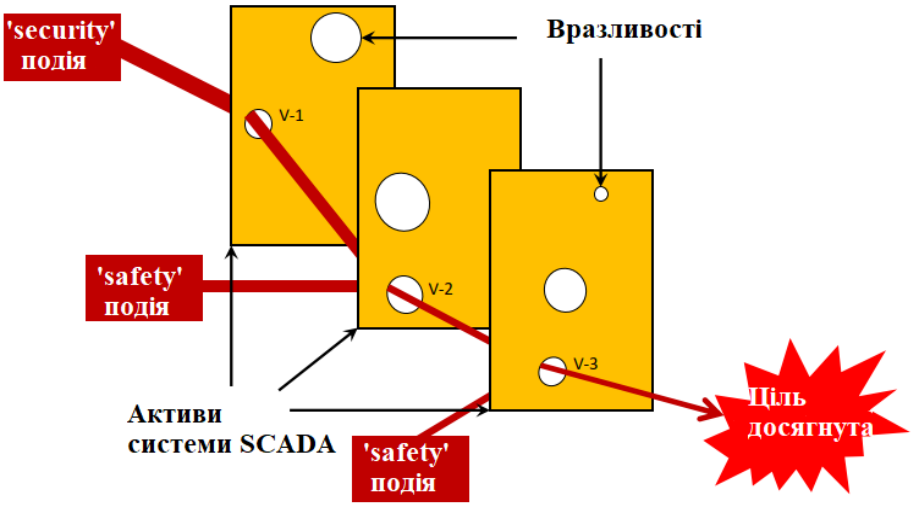


Рисунок 3.3 – Приклад сценарію небажаних подій

Як приклад можна навести наступний сценарій, недотримання працівником підприємства, в якому функціонує SCADA система, вимог для налаштування паролей може привести до реалізації атаки підбору паролів за допомогою відомих утиліт.

3.1.2 Оцінка функції правдоподібності

Фінальна оцінка правдоподібності сценарію небажаних подій, який включає в себе події, пов’язані з ‘safety’ та з ‘security’буде одна.

Проте, незважаючи на це, для сценаріїв небажаних подій, пов’язаних з ‘safety’ та з ‘security’, функцію правдоподібності спочатку необхідно розраховувати окремо. Оскільки джерела ризику для ‘safety’ та ‘security’ мають різний характер. Як правило, правдоподібність небажаних подій направлених на ‘safety’ набагато нижча в порівнянні з правдоподібністю реалізованих атак на основі спрямованих на порушення ‘security’. Тому, будемо розглядати дві різних шкали для оцінювання правдоподібності небажаних сценаріїв/атак.

Отже, важливо пам’ятати, що в фінальний сценарій можуть входити різні комбінації небажаних подій, пов’язаних з ‘safety’ та з ‘security’. Зважаючи на це, можна виділити 3 типи сценаріїв з подіями :

- сценарії, які містять події, які пов'язані лише з ‘safety’;

- сценарії, які містять події, які пов'язані лише з ‘security’;
- сценарії, які містять події, які пов'язані з ‘safety’ та ‘security’.

3.1.2.1 Оцінка правдоподібності реалізації ‘safety’ подій

Якісна оцінка правдоподібності для небажаних подій направлених на ‘safety’ поділяється на 6 типів в залежності від кількісної оцінки правдоподібності:

- ‘не застосовно’ – у випадку, коли сценарій небажаних подій містить події, які пов’язані з ‘security’ та не пов’язані з safety;
- дуже малоймовірна подія – у випадку, коли сценарій небажаних подій містить подію, яка є практично неможливою, тобто дуже малий шанс її реалізації;
- середньо ймовірна подія – у випадку, коли сценарій небажаних подій містить подію, яка трапляється рідко;
- ймовірна подія - у випадку, коли сценарій небажаних подій містить подію, яка час від часу;
- дуже ймовірна подія - у випадку, коли сценарій небажаних подій містить подію, яка дуже часто трапляється.

Детальнішу класифікацію можна побачити в таблиці 3.2.

Таблиця 3.2 - Рівні оцінки правдоподібності для небажаних подій, пов’язаних з ‘safety’

Оцінка правдоподібності ‘safety’ події	**Опис**	**Кількісне значення функції правдоподібності**
N/A	‘Не застосовно’	0
E	Дуже малоймовірна подія	$0 \leq P_e \leq 0,2$
D	Малоймовірна подія	$0,2 < P_e \leq 0,4$

Продовження таблиці 3.2

C	Середньо ймовірна подія	$0,4<P_e\leq0,6$
B	Ймовірна подія	$0,6<P_e\leq0,8$
A	Дуже ймовірна подія	$0,8<P_e\leq1$

Якщо сценарій містить в собі декілька небажаних подій, пов'язаних з 'safety', то загальна функція правдоподібності для цих подій буде дорівнювати мінімальному значенню функції правдоподібності, яке є у подій в даному сценарії.

Кількісне значення функції правдоподібності для події, пов'язаної з 'safety' може розраховуватись 3 способами, в залежності від типу події, для якої обчислюється дана функція, а саме:

- якщо подія пов'язана з відсутністю/наявністю налаштувань безпеки SCADA системи – то у такому випадку складається дві наступних 5-рівневих критеріальних шкали, на основі яких буде визначено відповідне кількісне та якісне значення функції правдоподібності:
  - шкала відповідності встановлених налаштувань безпеки до найкращих практик безпеки. Результатом оцінки буде величина R_1;
  - шкала відповідності встановлених налаштувань безпеки до документації підприємства. Результатом оцінки буде величина R_2.

  Важливим моментом є те, що дані шкали не рівнозначні з точки зору впливу на оцінку функції правдоподібності, оскільки критерій наявності налаштування в системі є набагато важливішим за наявність документально-описаних налаштувань у відношенні 80%/20%. Відповідно коефіцієнти біля значень R_1 та R_2 у формулі розрахунку оцінки правдоподібності будуть відповідно мати значення 0,8 та 0,2. Варто зважати також на той факт, що функція правдоподібності є оберненою до оцінки відповідності до критеріїв, оскільки високий рівень відповідності налаштувань безпеки критеріям означає низький рівень реалізації небажаної події, пов'язаної з критеріями безпеки. Тому, вона буде обчислюватись за формулою:

$$P_{sa} = 1{,}2 - (0{,}8R_1 + 0{,}2R_2) \quad (3.1)$$

де P_{sa} – оцінка функції правдоподібності ‘safety’ події;

R_1 – оцінка відповідності налаштування безпеки до найкращих практик безпеки;

R_2 – оцінка відповідності налаштування безпеки до документації підприємства.

- якщо подія пов’язана з відсутністю/наявністю регламентуючої ІБ та ІТ-процеси документацією на підприємстві – то складається 5-рівнева критеріальна шкала, на основі якої буде визначено відповідне кількісне та якісне значення функції правдоподібності. Результатом оцінки згідно шкали буде величина R_1 і функція правдоподібності обчислюватиметься за формулою:

$$P_{sa} = 1{,}2 - R_1 \quad (3.2)$$

де P_{sa} – оцінка функції правдоподібності ‘safety’ події;

R_1 – оцінка якості розробленої документації.

- якщо ‘safety’ подія зв’язана з функціонуванням ІТ та ІБ-процесів, які відбуваються на постійній основі (щоденно, щотижнево, і т.д.) та відповідно в результаті виконання процесу кожного разу формуються артефакти, які можна перевірити – то у такому випадку складається популяція артефактів за певний проміжок часу, з якої формується вибірка згідно правил описаних в таблиці 3.3. Правила описані в таблиці згідно міжнародної методології аудиту, яка використовується при тестуванні великих наборів даних. Вибірка перевіряється для того, щоб можна було оцінити ефективність функціювання процесу. Функція правдоподібності визначається на основі перевіреної вибірки, вона аналогічно вище описаним формулам є протилежною до оцінки ефективності процесу. Результатом оцінки ефективності процесу буде величина R_1, яка обчислюється за формулою:

$$R_1 = \frac{n_e}{n_s} \quad (3.3)$$

де R_1 – оцінка ефективності функціонування ІТ/ІБ процесу;

n_e - кількість значень артефактів, які відповідають усім вимогам процесу;

n_s - кількість значень артефактів, які були отримані в результаті виконання процесу (кількість артефактів, які потрапили у вибірку).

Функція правдоподібності у такому випадку обчислюватиметесь за формулою:

$$P_{sa} = 1 - R_1 \quad (3.4)$$

де P_{sa} – оцінка функції правдоподібності ‘safety’ події;

R_1 – оцінка ефективності функціонування ІТ/ІБ процесу.

Таблиця 3.3 - Правила формування вибірки для тестування процесу

№	Кількість значень в популяції	Кількість значень вибірки
1	0	0
2	Від 1 до 5	Вся популяція
3	Від 5 до 50	5
4	Від 50 до 250	10% від популяції
5	Більше 250	25

Наприклад: нехай подія, пов’язана з ‘safety’ – це ‘в результаті того, що пароль аккаунта адміністратора SCADA системи містить 4 символи, аккаунт було скомпрометовано’. Даний випадок підпадає під першу категорію та функція правдоподібності буде визначатись на основі розроблених критеріальних шкал. У даному випадку можна розглядати 2 критеріальних шкали:

- Шкала складності паролю встановленого в системі паролю та відповідності його до найкращих практик безпеки. Приклад шкали зображено у таблиці 3.4.
- Шкала відповідності встановленого в системі паролю згідно регламентуючої документації підприємства. Приклад шкали зображено у таблиці 3.5.

Таблиця 3.4 – Шкала складності встановлених парольних налаштувань

№	Якісне значення відповідності паролю до найкращих практик безпеки	Опис складності парольних налаштувань	Кількісне значення
1	Дуже низький рівень парольних налаштувань	Мінімальна довжина паролю ≤ 2 символів	0,2
2	Низький рівень парольних налаштувань	Мінімальна довжина паролю $\in (2; 4]$ символів	0,4
3	Середній рівень парольних налаштувань	Мінімальна довжина паролю $\in (4; 7]$ символів	0,6
4	Високий рівень парольних налаштувань	Мінімальна довжина паролю $\in (7; 10]$ символів	0,8
5	Дуже високий рівень парольних налаштувань	Мінімальна довжина паролю ≥ 10 символів	1

Таблиця 3.5 – Шкала складності парольних налаштувань відповідно до регламентуючої документації

№	Якісне значення відповідності	Опис	Кількісне значення
1	Дуже низький рівень	Відсутність встановлених парольних налаштувань та регламентуючої документацій, яка визначає вимоги до парольних налаштувань	0,2
2	Низький рівень	Наявність задокументованих парольних налаштувань, проте відсутність встановлених парольних налаштувань системі	0,4

Продовження таблиці 3.5

3	Середній рівень	Наявність встановлених парольних налаштувань системі, проте відсутність задокументованих парольних налаштувань	0,6
4	Високий рівень	Встановлені парольні налаштування не відповідають парольним налаштуванням, визначених в документації	0,8
5	Дуже високий рівень	Встановлені парольні налаштування відповідають парольним налаштуванням в системі	1

Наприклад: нехай подія, пов’язана з ‘safety’ – це ‘в результаті некоректної видачі прав доступу до SCADA системи, працівник підприємства отримав надмірні права, що призвело до розкриття конфіденційної інформації’. Даний випадок підпадає під третю категорію та функція правдоподібності в такому випадку буде визначатись на основі тестування вибірки. Оскільки процес видачі доступу до SCADA системи є постійним, то необхідно сформувати популяцію працівників, яким видавались права за 2019 рік та список прав, які надавались для цих працівників. Нехай сформована популяція містить 215 працівників. Оскільки 215 це менше ніж 250 та більше ніж 50, то вибірка буде складатись зі 22 працівників, яким видавались права. Далі необхідно рандомно вибрати 22 працівника з 215 та перевірити чи права, які були видані для них відповідають списку прав, які були запрошені. В результаті перевірки було виявлено, що для 20 працівників з 22 права були видано належним чином, згідно запрошеним. Відповідно, розраховуємо і отримуємо, що $R=\frac{20}{22}=0{,}9$, відповідно, $P_{sa}= 0{,}1$, що в свою чергу означає, що правдоподібність реалізації небажаного сценарію з некоректною видачою прав доступу до системи SCADA є дуже малоймовірною (згідно таблиці 3.2).

3.1.2.2 Оцінка правдоподібності реалізації ‘security’ подій

Якісна оцінка правдоподібності для відомих атак, реалізованих на основі відомих вразливостей залежить від 2 факторів:

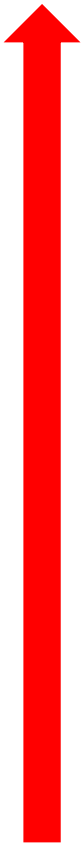
1. рівень вразливості: дана вразливість легко/важко реалізовується в залежності від існуючих превентивних заходів, які використовуються для попередження даної атаки. Приймемо за шкалу 3 наступних рівні вразливостей, які зображені та описані в таблиці 3.6:
   - Легкий рівень (E)
   - Середній рівень (M)
   - Важкий рівень (H)

Таблиця 3.6 – Рівень вразливості системи до відомих атак

Якісна шкала	**Рівень вразливості системи до атаки**	**Опис**
Експлуатація  **Ступінь важкості експлуатації вразливості**	**1**	**Легкий рівень (E):** немає запобіжних мір, які використовуються проти найрозповсюджених атак
	2	**Середній рівень (M):** частково існують запобіжні міри, які використовуються проти найрозповсюджених атак
	3	**Важкий рівень (H):** запобіжні міри, які використовуються проти найрозповсюджених атак постійно переглядаються та покращуються

2. Рівень необхідних технічних знань та використання технічних засобів для реалізації атаки. Дана шкала складається з наступних 4 рівнів, які описані та представлені в таблиці 3.7:
    - Легкий рівень (T)
    - Середній рівень (M)
    - Складний рівень (D)
    - Дуже складний рівень (VD)

Таблиця 3.7 - Рівень важкості реалізації атак

Якісна шкала	**Рівень важкості реалізації атаки**	**Опис**
Важкість технічної реалізації атаки 	**1**	**Легкий рівень (T):** реалізація атаки вимагає знання мінімальних технічних навиків в області кібербезпеки та експлойти для даних атак є у відкритому доступі
	2	**Середній рівень (M):** реалізація атаки вимагає знання середніх технічних навиків в області кібербезпеки та експлойти для даних атак є у відкритому доступі
	3	**Складний рівень (D):** реалізація атаки вимагає поглиблених технічних знань в області кібербезпеки та додаткових доопрацювань існуючих експлойтів
	4	**Дуже складний рівень (VD):** реалізація атаки вимагає глибоких технічних знань в області кібербезпеки та самостійної розробки експлойтів

Після того, як було визначено особливості реалізації події, пов’язаної з ‘security’, необхідно визначити оцінку функції правдоподібності для даного типу подій.

Якісна оцінка функції правдоподібності небажаних подій, які виникли на основі реалізації атаки, визначається за допомогою матриці, в основі якої заложено 2 раніше отриманих оцінки: щодо рівню вразливості системи до атаки, яка розглядається і важкості реалізації даної атаки. Матриця відповідності представлена у вигляді таблиці 3.8.

Таблиця 3.8 - Рівень оцінки правдоподібності подій, пов’язаних з ‘security’

Якісна оцінка правдоподібності		**Важкість технічної реалізації атаки**			
		T	**M**	**D**	**VD**
Ступінь важкості експлуатації атаки	**E**	4	4	3	2
	M	4	3	2	1
	H	2	2	1	1

По-аналогії з оцінкою правдоподібності для подій, пов’язаних з ‘safety’, якщо сценарій містить в собі декілька небажаних подій, пов’язаних з ‘security’, то загальна функція правдоподібності для цих подій буде дорівнювати мінімальному значенню функції правдоподібності, яке є у ‘security’ подій в даному сценарії.

Якщо переводити якісний рівень оцінки правдоподібності небажаних подій, пов’язаних з ‘security’ у кількісний, то отримаємо значення, які представленні в таблиці 3.9

Таблиця 3.9 - Рівень оцінки правдоподібності подій, пов’язаних з ‘security’

Рівень оцінки правдоподібності ‘security’ події	**Опис**	**Кількісне значення функції правдоподібності**
N/A	‘Не застосовно’	0
1	Низький	$0<x\leq0,25$
2	Середній	$0,25<x\leq0,5$
3	Високий	$0,5<x\leq0,75$
4	Дуже високий	$0,75<x\leq1$

Проте, кількісну оцінку правдоподібності можна визначити не лише через якісну оцінку. Для оцінки правдоподібності можна використовувати статистику, яка відображає відсоток систем вразливих до таких типів атак. Такий метод рекомендується застосовувати лише у тому випадку, якщо немає достатньо ресурсів та можливості, щоб перевірити систему повноцінним методом.

Приклад такої оцінки відображено в таблиці 3.10. Дана оцінка була складена на основі статистики, яка була представлена в CyberX 2019 Global ICS & IIoT Risk Report.

Таблиця 3.10 - Функція правдоподібності

Назва атаки	**Оцінка функції правдоподібності**
Переповнення буферу	0,84
Атака відмови в обслуговуванні (DoS)	0,53
Пошкодження пам’яті	0,84
Модифікація повідомлень	0,57
Модифікація логіки трапу	0,4
Атака відмови в обслуговуванні (DDOS)	0,84

Продовження таблиці 3.10

Неавторизоване виконання команд	0,84
Спуфінг (Spoofing)	0,4
Атака підбору паролів	0,69

3.1.2.3 Оцінка правдоподібності реалізації сценарію

Отже, після того, як були оцінені події пов’язані з ‘safety’ і ‘security’ окремо, було отримано наступні оцінки:

- Події, які пов'язані лише з ‘safety’ мають правдоподібність (P_{sa}, N/A)
- Події, які пов'язані лише з ‘security’ мають правдоподібність (N/A, P_{se})
- Події, пов'язані з ‘safety’ та ‘security’ мають правдоподібність (P_{sa}, P_{se}).

При розрахунку кількісної оцінки правдоподібності реалізації сценарію, який містить події, пов’язані з ‘safety’ та ‘security’ необхідно застосовувати наступну формулу [6]:

$$P_k = min<P_{sa}, P_{se}> \quad (3.5)$$

де $k \in \lfloor 1, n \rfloor$,

n-кількість сценаріїв небажаних подій, які розглядаються при оцінці;

P_k- результат функції правдоподібності появи *S(sa, se)*, де *se* та *sa* пов'язані відповідно з ‘safety’ та ‘security’;

P_{sa}- результат функції правдоподібності появи подій, пов’язаних з ‘safety’;

P_{se}- результат функції правдоподібності появи подій, пов’язаних з ‘security’.

Для загальної кількісної оцінки правдоподібності також є своя шкала, яка зображена в таблиці 3.11:

Таблиця 3.11 - Загальна оцінка функції правдоподібності сценарію

Оцінка правдоподібності сценарію	**Опис**	**Кількісне значення функції правдоподібності**
VL	Дуже низький	0<x≤0,2
L	Низький	0,2<x≤0,4
M	Середній	0,4<x≤0,6
H	Високий	0,6<x≤0,8
VH	Дуже високий	0,8<x≤1

Якщо в результаті оцінювання функцій правдоподібності подій ‘safety’ та ‘security’ були отримані лише якісні оцінки, то для обчислення правдоподібності сценарію, який містить ‘safety’ та ‘security’ події застосовується матриця, яка зображена в таблиці 3.12, де відповідно:

- VL - дуже низька оцінка функції правдоподібності;
- L - низька оцінка функції правдоподібності;
- M - середня оцінка функції правдоподібності;
- H - висока оцінка функції правдоподібності;
- VH – дуже висока оцінка функції правдоподібності.

Якісна оцінка правдоподібності реалізації сценарію, який містить події, пов’язані з ‘safety’ та ‘security’ буде визначатися як клітка матриці, яка знаходить на перетині значень оцінки правдоподібності ‘safety’ події та ‘security’ події відповідно:

$$P_k = P_{sase} \tag{3.6}$$

де $k \in \lfloor 1, n \rfloor$, n-кількість сценаріїв небажаних подій, які розглядаються при оцінці;

P_{sa}- результат функції правдоподібності появи подій, пов’язаних з ‘safety’;

- P_{se}- результат функції правдоподібності появи подій, пов'язаних з 'security'.

Таблиця 3.12 - Оцінка правдоподібності сценарію небажаних подій

Оцінка правдоподібності сценарію		**Рівень оцінки правдоподібності для 'safety'подій**					
		E	**D**	**C**	**B**	**A**	**N/A**
Рівень оцінки правдоподібності для 'security'подій	**N/A**	VL	L	M	H	VH	N/A
	4	VL	L	M	H	VH	VH
	3	VL	L	M	H	H	H
	2	VL	L	M	M	M	H
	1	VL	L	L	L	L	M

Варто зважати на те, що отримана кількісна оцінка рівня правдоподібності є більш точною ніж якісна.

3.1.3 Оцінка збитків

Компрометація SCADA систем може привести до завдання шкоди не тільки підприємству, де функціонує SCADA систем, але і до виникнення надзвичайної ситуації регіонального чи міжнародного характеру та до інших істотних негативних наслідків в соціальній, політичній, економічній, військовій чи інших сферах діяльності.

Взагалі, оцінку збитку можна проводити на основі одного з трьох нижчевказаних способів:

- завчасна оцінка збитку;
- апостеріорна прогнозна оцінка збитку;

- оцінка збитку на основі фактичних даних.

Завчасна оцінка основується на аналізі та оцінці процесів формування факторів впливу на виникнення небажаних наслідків. В даному випадку враховуються всі можливі випадки, які можуть бути отримані при реалізації сценарії небажаних подій/атак на систему.

Оцінка за фактичними даними будується на основі аналогічних аварій, що сталися на підприємстві, або на основі аварій в аналогічній галузі.

Особливий інтерес представляє собою апостеріорна прогнозна оцінка, яка дає хорошу основу для прийняття досить конкретних рішень щодо забезпечення безпеки SCADA системи. При апостеріорного прогнозному підході слід проводити інтегральну оцінку збитку, яка включає в себе такі складові, як: людські втрати, погіршення екологічної обстановки, матеріальні і фінансові втрати. Наслідки аварії представляють собою ланцюг послідовних взаємопов'язаних подій. Число ланок в цьому ланцюзі може бути досить велике. Вони різноманітні і мають економічну, соціальну, екологічну та навіть політичну складові. Однак в більшості випадів першочерговою є економічна складова, яка представляє собою сукупний збиток, понесений людьми в результаті виникнення аварійної ситуації, а також сумарні витрати, не пов'язані з компенсацією збитків.

При вимірі збитку немає універсальної шкали його оцінки. В основному використовуються абсолютна і відносна. Абсолютна шкала, як правило, є кількісною. У них застосовуються стандартні значення величин, наприклад вартість основних фондів підприємства, конкретна кількість нещасних випадків, що сталися за той чи інший період. Суб'єктивні шкали створюються тоді, коли немає конкретних кількісних даних для визначення збитку.

В даній роботі буде представлена відносна оцінка збитків, яка характеризується якісними показниками. Тому, оцінка збитків - це якісна міра, яка характеризує наслідки, отримані в результаті здійснення небажаного сценарію подій, пов’язаних зі ‘safety’ та/або реалізації атаки на відому вразливість SCADA системи (події, пов’язані з ‘security’).

Якісна шкала оцінки збитків може бути розподілена наступним чином:

- дуже низький збиток;
- низький збиток;
- середній збиток;
- високий збиток;
- дуже високий збиток.

Дуже низький рівень збитку передбачає в результаті реалізації сценарію небажаних подій настання наслідків, пов’язаних з несправністю SCADA системи, що не впливає на підприємство в цілому та може бути виправлено протягом незначної кількості часу. Наслідки є оборотними.

Низький рівень збитку передбачає в результаті реалізації сценарію небажаних подій настання наслідків, пов’язаних з несправністю SCADA системи, що може частково впливати на інші процеси підприємства, що не є критичними та може бути виправлено протягом незначної кількості часу. Наслідки є оборотними.

Середній рівень збитку передбачає в результаті реалізації сценарію небажаних подій настання наслідків, пов’язаних з SCADA системою, що впливають на роботу підприємства та може бути виправлено протягом декількох годин. Наслідки є оборотними.

Високий рівень збитку передбачає в результаті реалізації сценарію небажаних подій настання наслідків, пов’язаних з SCADA системою, що впливають на роботу інших підприємств/установ/сфер, які пов’язані з підприємством, на якому функціонує SCADA система та може бути виправлено протягом декількох годин. Наслідки є необоротними.

Дуже високий рівень збитку передбачає в результаті реалізації сценарію небажаних подій настання наслідків, пов’язаних з SCADA системою, що впливають на здоров’я та життя людей, екологічний стан. Наслідки в такому випадку є необоротними.

Більш точний опис рівнів буде варіюватись в залежності від роду діяльності підприємства, на якому функціонує SCADA система.

На прикладі енергосистеми нижче в таблиці 3.13 продемонстровано варіант опису рівнів збитку.

Таблиця 3.13 – Рівні збитку

Рівень збитку	**Назва рівня збитку**	**Опис**
1	Дуже низький	Реалізація сценарію небажаних подій, призвела до незначних порушень SCADA системи, що були вирішені IT- спеціалістами в рамках однієї години
2	Низький	Реалізація сценарію небажаних подій, призвела до незначних порушень SCADA системи, що стало причиною відсутності енергопостачання протягом декількох хвилин на підприємстві
3	Середній	В наслідок порушення працездатності SCADA системи, була призупинена робота підприємства, що стало причиною значних фінансових втрат
4	Високий	В наслідок порушення працездатності SCADA системи, було відсутнє енергопостачання протягом 4 годин у одній із областей, що привело до зупинки інших підприємств що в свою чергу сталою причиною значних фінансових втрат.
5	Дуже високий	В наслідок порушення працездатності SCADA системи, було відсутнє енергопостачання у населених пунктах, у військових госпіталях, у лікарнях протягом доби у одній із областей, що привело до людських втрат.

Кількісна оцінку збитків представлена на основі якісної оцінки у вигляді граничних значень від 0,2 до 1 у таблиці 3.14.

Таблиця 3.14 – Оцінка рівнів збитку

Рівень збитку	**Назва рівня збитку**	**Кількісне значення оцінки збитку**
1	Дуже низький	0,2
2	Низький	0,4
3	Середній	0,6
4	Високий	0,8
5	Дуже високий	1

Після отримання всіх необхідних результатів загальна оцінка рівня збитку отриманого в наслідок реалізацію сценарію визначається як максимальне отримане значення збитку для розглянутих подій, які входять в сценарій.

3.1.4 Визначення ризику, пов'язаного з параметрами ‘safety’ та ‘security’ SCADA системи

Для початку необхідно представити визначення ризиків, пов'язаних з ‘safety’ та ‘security’. В подальшому ці два окремих ризики будуть використані для оцінки загального ризику направленого на систему SCADA.

Ризик, пов'язаний з ‘safety’ SCADA, представимо у вигляді функції від 3 змінних [6]:

$$R_{safety} = (S_{sai}, P_{sai}, X_{sai}), \quad (3.7)$$

де $i = 1, 2, ..., N$;

R_{safety} - ризики, пов'язані з безпекою;

S_{sai} - опису сценарію виникнення небажаної події e та пов'язаних з цим наслідків;

P_{sai} - правдоподібність виникнення S;

X_{sai} – збиток, отриманий в наслідок реалізації S;

N - кількість можливих сценаріїв або небажаних подій, які направлені на ‘safety’ SCADA системи.

Ризик, пов'язаний з ‘security’ SCADA системи у контексті кібербезпеки - аналізується з точки зору функції правдоподібності та отриманих збитків при реалізації даної загрози, що в свою чергу використовує зарання відому вразливість SCADA системи. Він описується нижчевказанною формулою:

$$R_{security} = S_{sej}, P_{sej}, X_{sej} \quad (3.8)$$

де $j = 1, 2, ..., M$

$R_{security}$ - ризики, пов'язані з ‘security’ SCADA системи;

S_{sej} – опис сценарію порушення параметра ‘security’ SCADA;

X_{sej} – збиток, отриманий в наслідок реалізації сценарію, пов’язаного з ‘security’

M – кількість атак.

Використовуючи поняття ризиків, які описані вище –ризик від реалізації сценарію, який містить ‘safety’ та ‘security’ події обчислюється наступним чином:

$$R_i = (S (sa, se), P (sa, se), X (sa, se)) \quad (3.9)$$

де $i = 1, 2, ..., N;$

$S (sa, se)$ - опис сценарію виникнення небажаної події, що може призвести до інцидентів, пов’язаних з ‘safety’ та / або порушень пов’язаних з ‘security’

$P (sa, se)$- оцінка функції правдоподібності виникнення сценарію, який містить події, пов’язані з ‘safety’ та / або порушень пов’язаних з ‘security’

$X (sa, se)$ – збиток, отриманий в наслідок реалізації сценарію S (sa, se);

N - кількість можливих сценаріїв, які містять небажані події, пов’язані з ‘safety’ та ‘security’ системи SCADA.

3.1.4.1 Розрахунок ризику від реалізації небажаного сценарію подій

Оцінка ризику від реалізації небажаного сценарію подій ‘safety’ і ‘security’ розраховується добуток значення функції правдоподібності реалізації сценарію на збиток, який був отриманий як наслідок реалізації цього ж сценарію.

Якщо оцінки правдоподібності сценарію були отримані у якісному вигляді – то необхідно їх перевести згідно таблиці 3.11 у кількісні значення, взявши при цьому найбільше граничне значення певного рівня.

Зважаючи на вище сказане, формула 3.8 матиме наступний вигляд:

$$R_i = P_i \times X_i \qquad (3.10)$$

де $i \in \lfloor 1, n \rfloor$, n-кількість сценаріїв небажаних подій, які розглядаються при оцінці.

P_i- результат функції правдоподібності появи *S(sa, se)*, де *sa* та *se* пов'язані відповідно з ‘safety’ та ‘security’ події;

X_i- величина збитку, отриманого в результаті реалізації і-го сценарію;

R_i – величина ризику, отримана від реалізації і-го сценарію.

3.1.4.2 Усереднена оцінка ризику, отриманого від реалізації небажаних сценаріїв подій

Загальна оцінка ризику усіх сценаріїв розраховується як середнє значення від значень оцінки ризику, які було отримано для кожного сценарію окремо, оскільки всі сценарії є рівнозначними по своїх значимості. Дана величина обчислюється за формулою:

$$R = \frac{\sum_{i=1}^{n} R_i}{n} \qquad (3.11)$$

де і $\in \lfloor 1, n \rfloor$, n-кількість сценаріїв небажаних подій, які розглядаються при оцінці.

R_i- величина ризику, отримана від реалізації і-го сценарію;

R- усереднена оцінка ризику від реалізації усіх небажаних сценаріїв.

На основі отриманої оцінки R обчислюємо рівень захищеності SCADA системи вцілому.

3.2 Розрахунок оцінки захищеності SCADA системи

Використання інформаційних систем і технологій пов'язано з певною сукупністю ризиків. Оцінка ризиків, перш за все, необхідна для контролю ефективності діяльності цих систем в області інформаційної безпеки, прийняття цільових заходів і створення економічно - ефективних заходів для захисту системи. Важливо пам’ятати, що добросовісно виконана і ретельно проведена перша оцінка може істотно полегшити подальшу діяльність, зв’язану з забезпеченням безпеки системи.

Тому, при розрахунку оцінки захищеності системи оцінка ризиків відіграє важливу роль, оскільки величина «захищеності» є діаметрально протилежною величині «ризику» і обчислюється за формулою:

$$SE = (1 - \sqrt{R}) \times 100\%, \quad (3.11)$$

SE – рівень захищеності SCADA системи;

R- загальний ризик, пов’язаний з параметрами ‘safety’ та ‘security’ SCADA системи;

Зважаючи на той факт, що R лежить в проміжку від [0;1], то отримуємо, що кількісна оцінка захищеності відповідно заходиться в межах від [0;100].

Щодо якісної оцінки – то після того як обчислено кількісну оцінку захищеності SCADA системи можна визначити рівень його захищеності і якісно. Шкала якісної оцінки захищеності варіюється наступним чином

- 0-25% - низький рівень захищеності системи;
- 26-75% - середній рівень захищеності системи;
- 76-100% - високий рівень захищеності системи.

3.3 Практичне застосування підходу до оцінки захищеності

Для того, щоб захистити SCADA систему, необхідно знати, які вразливості можуть призвести до компрометації системи, щоб в подальшому виправити їх та

не дати можливості зловмисникам ними скористатись. В даному випадку для перевірки SCADA системи було використано підхід до оцінки захищеності SCADA системи на основі функції правдоподібності.

Для перевірки на основі розробленого підходу було обрано Siemens SCADA систему підприємства А. Дані, які використовувались для тестування та оцінки подій, пов'язаних з 'safety' було отримано згідно договору, підписаного з Компанією А. В результаті оцінки встановлено рівень захищеності SCADA системи. Проміжні результати для визначення загальної оцінки захищеності SCADA для переліку нижче вказаних сценаріїв небажаних подій, проілюстровано в таблиці 3.15:

1. не виконання умов обслуговування SCADA системи третіми особами може привести до отримання неавторизованого доступу до SCADA системи сторонніми особами та виведення з експлуатації серверів системи на невизначений період часу (обслуговування серверів здійснюється згідно з усіма вимогами безпеки);
2. некоректна видача доступу до приміщення, в якому розташовані сервери SCADA системи, може привести до несанкціонованого доступу персоналу до заборонених зон та відключення системи. (3 з 8 людям видано не коректно доступ);
3. відсутність стійких парольних налаштувань може привести до компрометації облікового запису працівника та отримання неавторизованого доступу до SCADA системи (парольні налаштування 6 символів) та викрадення конфіденційної інформації;
4. відсутність стійких парольних налаштувань може привести до компрометації облікового запису працівника, отримання неавторизованого доступу до SCADA системи (парольні налаштування 6 символів) та встановлення шкідливого ПЗ;
5. відсутність періодичного резервного копіювання може привести до втрати усіх конфіденційних даних, які зберігались у SCADA системі;

6. відсутність чітких сроків реагування на інциденти може привести до невчасного виявлення вирішення інцидентів та втрати важливих даних, які зберігаються в SCADA системі чи до отримання неавторизованого повного доступу на рівні SCADA систем;
7. відсутність обмеженого доступу до логів системи з діями користувачів може стати причиною приховання неправомірних дій зі сторони Адміністраторів SCADA системи;
8. відсутність обмежень для TCP порта 777/наявність вразливості ПЗ SCADA системи може стати причиною переповнення буфера;
9. використання застарілого програмного забезпечення може стати причиною DOS атаки;
10. реалізація Spoofing атаки на основі відомих експлойтів;
11. в результаті вразливого ПЗ SCADA системи можна реалізувати атаку «модифікація повідомлень»;
12. відсутність властивостей безпеки аутентифікації в протоколі DNP3 є причиною реалізації DDOS атаки, що в свою чергу може привести до привести до втрати даних чи втрати функціональності системою;
13. в результаті вразливого ПЗ SCADA системи можна реалізувати атаку «Modifying Ladder Logic»;
14. в результаті вразливого ПЗ SCADA системи можна реалізувати атаку «Unauthorization code execution»;
15. встановлення шкідливого програмного забезпечення на сервери, де розміщена SCADA система може привести до реалізації DDOS атаки;
16. встановлення шкідливого програмного забезпечення на сервери, де розміщена SCADA система може привести до реалізації атаки «Unauthorization code execution»;
17. відсутність гарячого резервного копіювання продуктивних серверів, на яких розміщена SCADA система може привести до критичної ситуації у

випадку порушення функціональності продуктивних серверів, на яких розміщена SCADA система;

18. некоректна видача доступу до SCADA системи, може привести до несанкціонованому доступу персоналу до конфіденційних даних та їх розголошення. (14 з 16 людям видано коректно доступ);
19. доступ звільнених осіб до приміщення, в якому розташовані сервери SCADA системи, не був вчасно забраним, що може привести до несанкціонованому доступу до серверів (доступ був забраний вчасно для всіх звільнених, хто мав доступ до системи);
20. доступ звільнених осіб до системи SCADA не був вчасно забраним, що може привести до несанкціонованому доступу до конфіденційної інформації та її розголошення (1 з 10 людей невчасно забраний доступ);
21. відсутність стадії тестування нового функціоналу, який добавляється в систему може привести до неправильного функціонування системи/невчасного виявлення закладеного шкідливого ПО, що в свою чергу може привести до порушення діяльності системи в цілому (тестування проводилось для 8 змін з 10);
22. впровадження неавторизованого функціоналу в систему може привести до неправильного функціонування системи/невчасного виявлення закладеного шкідливого ПО, що в свою чергу може привести до порушення діяльності системи в цілому (9 змін з 10 були авторизовані);
23. наявність доступу в розробників SCADA на продуктивні сервера може привести до внесення неавторизованих змін у функціонал системи та використання цієї можливості у власних інтересах (1 з 5 розробник).

Таблиця 3.15 - Проміжні результати оцінки захищеності SCADA системи

Номер сценарію небажаної події	Оцінка правдоподібності ‘safety’ події (P_{sai})	Оцінка правдоподібності ‘security’ події (P_{sej})	Загальна оцінка правдоподібності ‘safety’ подій (P_{sa})	Загальна оцінка правдоподібності ‘security’ подій (P_{se})	Оцінка правдоподібності небажаного сценарію подій (P_i)	Оцінка рівня збитку від реалізації сценарію (X_i)	Оцінка ризику від реалізації небажаного сценарію (R_i)
1	0,2 (E)	N/A	0,2 (E)	N/A	0,2 (VL)	0,8 (4 рівень)	0,16
2	0,375 (D)	N/A	0,375 (D)	N/A	0,375 (D)	0,2 (1 рівень)	0,075
3	0,6 (C)	N/A	0,6 (C)	N/A	0,6 (M)	0,8 (4 рівень)	0,48
(4,5)	0,6 (C) 0,2 (E)	N/A	0,2 (E)	N/A	0,2 (VL)	0,8 (4 рівень)	0,16
(4,15)	0,6 (C)	0,4 (2)	0,6 (C)	0,4 (2)	0,4 (L)	1 (5 рівень)	0,4
(4,16)	0,6 (C)	0,84 (4)	0,6 (C)	0,84 (4)	0,6 (M)	1 (5 рівень)	0,6
6	0,2 (E)	N/A	0,2 (E)	N/A	0,2 (VL)	1 (5 рівень)	0,2
7	0,2 (E)	N/A	0,2 (E)	N/A	0,2 (VL)	0,6 (3 рівень)	0,12
8	N/A	0,84 (4)	N/A	0,84 (4)	0,84 (VH)	1 (5 рівень)	0,84
9	0,2 (E)	0,53 (3)	0,2 (E)	0,53 (3)	0,2 (VL)	1 (5 рівень)	0,2
10	N/A	0,4 (2)	N/A	0,4 (2)	0,4 (L)	1 (5 рівень)	0,4
11	N/A	0,57 (3)	N/A	0,57 (3)	0,57 (M)	0,2 (1 рівень)	0,114
12	N/A	0,84 (4)	N/A	0,84 (4)	0,84 (VH)	1 (5 рівень)	0,84

Продовження таблиці 3.15

13	N/A	0,4 (2)	N/A	0,4 (2)	0,4 (H)	0,2 (4 рівень)	0,08
14	N/A	0,84 (4)	N/A	0,84 (4)	0,84 (VH)	1 (5 рівень)	0,84
(4,16,15)	0,6 (C)	0,84 (4) 0,4 (2)	0,6 (C)	0,4 (2)	0,4 (L)	1 (5 рівень)	0,4
17	1 (A)	N/A	1 (A)	N/A	1 (VH)	1 (5 рівень)	1
18	0,125 (E)	N/A	0,125 (E)	N/A	0,125 (VL)	0,8 (4 рівень)	0,1
19	0 (E)	N/A	0 (E)	N/A	0 (VL)	0,2 (1 рівень)	0
20	0,1 (E)	N/A	0,1 (E)	N/A	0,1 (VL)	0,8 (4 рівень)	0,08
21	0,2 (E)	N/A	0,2 (E)	N/A	0,2 (VL)	1 (5 рівень)	0,2
(21,15)	0,2 (E)	0,84 (4)	0,2 (E)	0,84 (4)	0,2 (VL)	1 (5 рівень)	0,2
(21,16)	0,2 (E)	0,4 (2)	0,2 (E)	0,4 (2)	0,2 (VL)	1 (5 рівень)	0,2
(21,8)	0,2 (E)	0,84 (4)	0,2 (E)	0,84 (4)	0,2 (VL)	1 (5 рівень)	0,2
(21,15,16)	0,2 (E)	0,84 (4) 0,4 (2)	0,2 (E)	0,4 (2)	0,2 (VL)	1 (5 рівень)	0,2
22	0,1 (E)	N/A	0,1 (E)	N/A	0,1 (VL)	1 (5 рівень)	0,1
(22,15)	0,1 (E)	0,84 (4)	0,1 (E)	0,84 (4)	0,1 (VL)	1 (5 рівень)	0,1
(22,16)	0,1 (E)	0,4 (2)	0,1 (E)	0,4 (2)	0,1 (VL)	1 (5 рівень)	0,1
(22,8)	0,1 (E)	0,84 (4)	0,1 (E)	0,84 (4)	0,1 (VL)	1 (5 рівень)	0,1
(22,15,16)	0,1 (E)	0,84 (4) 0,4 (2)	0,1 (E)	0,4 (2)	0,1 (VL)	1 (5 рівень)	0,1
23	0,2 (E)	N/A	0,2 (E)	N/A	0,2 (VL)	0,6 (3 рівень)	0,12

На основі отриманих оцінок ризиків для 31 сценарію небажаних подій, пов’язаних з ‘safety’ та ‘security’ було обчислено усереднене значення оцінки ризиків від реалізації усіх сценаріїв. Використовуючи формулу (3.10), було визначено, що R = 0,28.

Підсумкова оцінка захищеності SCADA системи була обчислена за формулою (3.11) та зображена на рисунку 3.4. В результаті отримано, що SE = 47,1%.

Отже, можна зробити висновок, що SCADA система, що перевірялась на основі розробленого підходу в даній роботі, має середній рівень захищеності.

Висновки до розділу 3

В даному розділі було представлено підхід до оцінки захищеності SCADA систем. Охарактеризовано кожен із її рівнів та приведено послідовність дій, які необхідно виконати при застосуванні даної моделі. Основними етапами підходу до оцінки захищеності є наступні етапи:

- розробка та аналіз сценаріїв небажаних подій, які пов’язані з ‘safety’ та ‘security’ SCADA системи;
- оцінка функції правдоподібності небажаних сценаріїв;
- оцінка збитку, отриманого компанією в наслідок реалізації сценарію небажаних подій;
- оцінка ризику, пов’язаного з реалізацією сценаріїв небажаних подій;
- розрахунок оцінки захищеності SCADA системи.

Зважаючи на те, що результатом перевірки може бути як кількісна так і якісна оцінка, отримана в результаті обчислень згідно формул чи матриць, які представлено в підході, то можна за допомогою наступної шкали визначити якісний рівень захищеності SCADA системи:

- 0-25% - низький рівень захищеності системи;
- 26-75% - середній рівень захищеності системи;
- 76-100% - високий рівень захищеності системи.

Також на практиці було перевірено захищеність Siemens SCADA системи підприємства А за допомогою підходу до оцінки захищеності SCADA систем на основі функції правдоподібності.

На рисунку 3.4 зображено результати оцінки захищеності SCADA системи. В кінцевому результаті було встановлено, що SE = 47,1%, тобто це означає, що SCADA система має середній рівень захищеності.

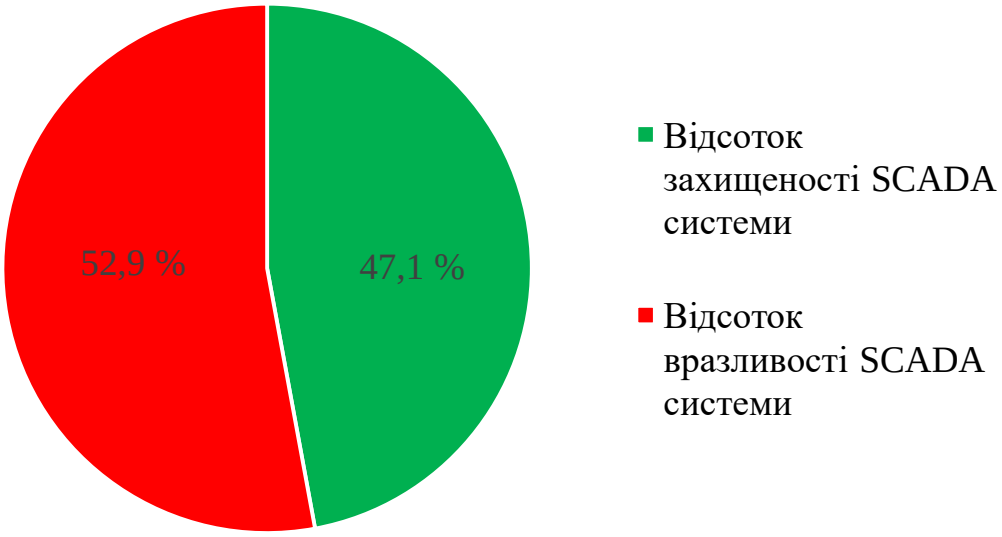


Рисунок 3.4 - Результати оцінки захищеності SCADA системи

ВИСНОВКИ

У минулому системи нагляду та збору даних SCADA використовувалися лише в системах розподілу нафти, газу та електроенергії. Сьогодні SCADA системи майже всюди: у телекомунікаційній, фармацевтичній та обробній промисловості. Плавне функціонування системи SCADA є життєво важливим не лише для безперебійної роботи секторів бізнесу, а також для навколишнього середовища і життя людини, оскільки будь-яке порушення може призвести до катастрофічних збитків.

З моменту з'єднання систем SCADA з Інтернетом, системи SCADA стали легкою мішенню для зловмисника. Це пов'язано з більш широкою поверхнею атаки і більшою кількістю векторів атаки на SCADA систему в цілому та її компоненти. Протягом останнього десятиліття SCADA системи неодноразово підлягали компрометації зі сторони зловмисників, проте був ряд атак, які мали дуже важкі наслідки. Наприклад, закриття атомного заводу Браунс Феррі в Алабамі через DDoS-атаку, вторгнення у водоочисні споруди в Харрісбергзі та Пенсільванії, зупинення багатьох залізничних ліній у східній частині США через вірус CSX Corp та реалізація вірусної атаки Stuxnet на великі енергетичні компанії, яка зіпсувала не лише програмний код та дані, а й самі реальні машини.

В результаті роботи було опрацьовано велику кількість необхідної літератури для кращого вивчення теми захищеності SCADA систем, особливо в таких областях, як атаки, вразливості та забезпечення захищеності SCADA систем. Встановлено, що кожен із способів перевірки стану їх безпеки має список переваг та недоліків. Звичайно, з кожним роком розроблюється все більша кількість підходів, методик, що вбирають в собі найкращі властивості попередніх варіантів, та в яких виправлені суттєві недоліки. Проте, зважаючи на загрози, що можливі для цих систем, зазвичай необхідно застосовувати комплекс перевірок. На даний момент не існує єдиного методу визначення рівня захищеності SCADA систем, який би дозволяв визначати проблеми з різних сторін.

В даній роботі представлено підхід до оцінки, який охоплює декілька аспек-

тів безпеки SCADA систем. Особливістю є те, що підхід до оцінки захищеності SCADA систем на основі функції правдоподібності було запропоновано вперше. Розроблений підхід направлений на визначення рівня захищеності SCADA системи, що перевіряється. Він основується на чотирьох основних етапах, на виході кожного з яких формуються кількісні/якісні дані, необхідні для обчислення оцінки захищеності SCADA системи.

В основі представленого підходу лежить аналіз SCADA системи не лише зі сторони здатності системи бути стійкою до відомих атак, а й зі сторони внутрішнього обслуговування системи працівниками підприємства, де SCADA система функціонує. Відповідно в роботі запропоновано різні шкали та критерії для оцінювання SCADA системи з цих двох сторін. В свою чергу отримані результуючі оцінки при оцінюванні стійкості системи до відомих атак та захищеності зі сторони ефективності функціонування внутрішніх IT та ІБ-процесів мають однаковий вплив на загальну оцінку захищеності SCADA системи.

Кінцеве значення, що характеризує рівень захищеності залежить від наступних критеріїв:

1. функції правдоподібності, що характеризується величиною P;
2. оцінки збитків, отриманих в наслідок реалізації сценаріїв небажаних подій. Характеризується величиною X.
3. оцінки ризиків. Характеризується величиною Risk (R).

Також в роботі було представлено практичне застосування розробленого підходу, а саме було оцінено стан захищеності Siemens SCADA системи та встановлено, що вона має середній рівень захищеності (47,1%).

Отже, на відміну від раніше запропонованих методів оцінки захищеності, які передбачали лише оцінку захищеності системи зі сторони зовнішніх атак, розроблений метод передбачає оцінку захищеності зі сторони не лише зовнішніх атак, а й зі сторони впливу внутрішніх IT та ІБ-процесів підприємства на безпечне функціонування SCADA системи.

ПЕРЕЛІК ДЖЕРЕЛ ПОСЛАНЬ

1. Левашов А. SCADA [Електронний ресурс] / А. Левашов. - Режим доступу до ресурса: http://www.tadviser.ru/index.php:Стаття: SCADA_ назначение_систем – 20.06.2016.
2. Шахновский Г. Безопасность Систем SCADA и АСУТП [Електронний ресурс] / Г. Шахновский. - Режим доступу до ресурса: http://www. security bridge.com/biblioteka/stati_po_bezopasnosti/bezopasnost_sistem_scada_i_ asutp - 17.08.2016.
3. Особенности SCADA в процессе управления [Електронний ресурс]. - Режим доступу до ресурса: https://helpiks.org/8-78205.html – 28.11.2016.
4. Positive Technologies. Безопасность промышленных систем в цифрах [Електронний ресурс] / Positive Technologies. – Режим доступу до ресурса: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/SCADA-analytics-rus.pdf – 2012.
5. Шевяков И.А Анализ актуальных уязвимостей SCADA систем [Текст] / И.А Шевяков, А.Н. Соколов. - Екатеринбург, 2017. - 4с.
6. Positive Technologies. Безопасность АСУ ТП [Електронний ресурс] / Positive Technologies. – Режим доступу до ресурса: https://www.ptsecurity. com/upload/corporate/ru-ru/analytics/ICS-Security2017-rus.pdf – 2017.
7. Зябкин В.С. Оценка защищенности автоматизированной системы управления технологическими процессами в организации коммунального хозяйства [Текст] / В.С. Зябкин, А.А. Бабенко – Москва, 2017. — 17 с.
8. Parves Kamal. Identifying and Scoring Vulnerability in SCADA Environments [Текст] / Parves Kamal, Abdullah Abuhussein – Ванкувер, 2017. - 17с.